IMPLEMENTACIÓN DE UN *SECURITY INFORMATION AND EVENT MANAGEMENT –SIEM–* EN EL COMANDO DE LA ARMADA NACIONAL. DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

JORGE ENRIQUE FERNÁNDEZ GRANADOS
JUAN HAROLD HERRERA KAIRUZ
JUAN CARLOS CAMILO GARCÍA

UNIVERSIDAD PILOTO DE COLOMBIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

IMPLEMENTACIÓN DE UN *SECURITY INFORMATION AND EVENT MANAGEMENT –SIEM–* EN EL COMANDO DE LA ARMADA NACIONAL. DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

JORGE ENRIQUE FERNÁNDEZ GRANADOS
JUAN HAROLD HERRERA KAIRUZ
JUAN CARLOS CAMILO GARCÍA

Trabajo de grado como requisito parcial para optar al título de Especialización en Seguridad Informática

Ingeniero Álvaro Escobar Escobar
Director Especialización en Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

Hoy en día, en cualquier empresa se ha constituido en una necesidad imprescindible, emplear las Tecnologías de la Información (TI) que apoyen y contribuyan al mejoramiento de los procesos de seguridad permitiendo a las organizaciones ser más competitivas y conservar su reputación. Sin embargo, dichos avances traen consigo riesgos y amenazas, que atentan contra la información de las organizaciones.

Muy a menudo se implementan servicios que apoyan a las organizaciones a proteger su información usando herramientas avanzadas que permiten la detección de amenazas, vulnerabilidades, monitoreo de las redes de datos, correlación de eventos, análisis y gestión de eventos que ocurren en las plataformas de tecnología entre otros, que representan costos elevados adicionales a la operación de las entidades.

Como medida de defensa las Fuerzas Militares de Colombia a través del Comando Conjunto Cibernético (CCOC) impartió órdenes e instrucciones para la protección de la información de la infraestructura tecnológica, para brindar protección a la información militar y así mismo gestionar los incidentes relacionados con la seguridad de la información.

Con base en estos preceptos, se ha decidido realizar este trabajo investigativo con el propósito de aunar esfuerzos en conjunto con la Armada Nacional con el fin de complementar los mecanismos de defensa cibernéticos existentes que beneficien el gobierno de la seguridad de la información dentro de la institución.

1. JUSTIFICACIÓN

Los documentos CONPES (Consejo Nacional de Política Económica y Social) 3701 del 14 de Julio de 2011 y 3854 de Seguridad Digital del 11 abril del 2016, emitidos por el Departamento Nacional de Planeación (DNP), describen los lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país[1]; debido a estos lineamientos y para proteger a los ciudadanos de los riesgos informáticos, el gobierno creó el Comando Conjunto Cibernético (CCOC) de las Fuerzas Militares que tiene la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio, con el objetivo de prevenir, proteger y neutralizar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales[2], defender la infraestructura crítica, desarrollar capacidades de neutralización y reacción frente a incidentes informáticos.

La Armada Nacional dentro de su misión de contribuir a la defensa de la nación a través del empleo efectivo de un poder naval flexible en los espacios marítimos, fluvial y terrestre bajo su responsabilidad, busca fortalecer sus mecanismos de defensa, con el propósito de cumplir la función constitucional y participar en el desarrollo del poder marítimo y a la protección de los intereses colombianos, por tal razón es necesario contar con una estrategia para monitorear, revisar, prevenir y contrarrestar amenazas y/o vulnerabilidades que puedan atentar contra la integridad, confidencialidad y disponibilidad de la información.

A través de este proyecto se implementará un SIEM: (*Security Information and Event Management*) para la Dirección de Tecnologías de la Información y Comunicaciones de la Armada Nacional de Colombia, en cumplimiento de las órdenes emitidas por la red nacional de CSIRTs (*Computer Security Incident Response Team*, Equipo de Respuesta ante Incidencias de Seguridad) y cuerpos de investigación, para facilitar y estrechar los lazos de cooperación y apoyo nacionales para la solución de incidentes de seguridad cibernética, a través de una plataforma con niveles altos de seguridad.

El *Security Information and Event Management* (SIEM) como tecnología que provee análisis de seguridad en tiempo real de aplicaciones hardware y redes, permitirá implementar y fortalecer el cumplimiento de los lineamientos anteriormente descritos.

[1] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL; DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa. Colombia, [en línea], 14 de julio de 2011. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

[2] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL; DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3854 Política Nacional de Seguridad Digital. Colombia, [en línea], 11 de abril de 2016. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

2. FORMULACIÓN DEL PROBLEMA

¿Qué mecanismo de seguridad podría ser implementado en La Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional, con el fin de correlacionar eventos de las diferentes plataformas y así tener una mayor visibilidad para proteger la información de los sistemas de comunicación e informáticos que se manejan al interior del Comando?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar un *Security Information and Event Management* (SIEM) para la Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional ("DITEL"), mediante el uso de herramientas de software libre y gratuitas, con el fin de brindar visibilidad en tiempo real de ataques a la infraestructura tecnológica y advertir su impacto para la toma de decisiones por parte del área de ciberseguridad de la Armada.

3.2 OBJETIVOS ESPECÍFICOS

Implementar una herramienta de software libre o de bajo costo que correlacione, priorice y asigne los riesgos informáticos potenciales por medio de la recolección de eventos de los componentes tecnológicos designados por la Armada Nacional de Colombia (ARC).

Brindar a la Armada Nacional por intermedio de la implementación de un SIEM, un panorama visible ante un eventual ataque informático.

Realizar un levantamiento de información de la plataforma tecnológica del Comando de la Armada Nacional con el fin de determinar los dispositivos tecnológicos que serán incluidos en el monitoreo de correlacionador de eventos a implementar.

Determinar los requerimientos técnicos necesarios para la implementación del SIEM de acuerdo a la información recolectada.

Elaborar un documento entregable correspondiente a manual de operación, dirigido a la División de informática de la Armada Nacional.

Presentar el impacto de los ataques por medio de categorías o alertas bajas, medias y altas, plasmadas en paneles gráficos que sirvan de apoyo para la toma de decisiones por parte del área de ciberseguridad de la ARC.

4. TIPO DE INVESTIGACIÓN

Para la realización de este proyecto el tipo de investigación apropiado es de tipo correlacional y explicativo, dado que el tema principal es la recolección de eventos de seguridad y su posterior escalamiento para brindar soluciones efectivas para mantener la integridad, la disponibilidad y la confidencialidad de la información en el Comando de la Armada Nacional de Colombia.

5. HIPÓTESIS

Hi = La Implementación de un *Security Information and Event Management* (SIEM) en la Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional, dará una mayor claridad sobre los eventos de seguridad que ocurren relacionados con seguridad de la información y los activos informáticos, con el fin de determinar las acciones preventivas y correctivas que se deben tomar.

Ho = La no Implementación de un *Security Information and Event Management* (SIEM) en la Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional, no dará una mayor claridad sobre los eventos de seguridad que ocurren relacionados con seguridad de la información y los activos informáticos, y no será posible determinar de manera oportuna las acciones preventivas y correctivas que se deben tomar.

6. VARIABLES

Implementación de un SIEM.

Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional.

Eventos de seguridad.

Seguridad de la información.

Activos informáticos.

Acciones preventivas.

Acciones correctivas.

7. MARCO TEÓRICO

7.1 ANTECEDENTES

La plataforma tecnológica del Comando de la Armada Nacional cuenta con un sistema de log de eventos que manifiestan su comportamiento a nivel de seguridad. Estos eventos con poca frecuencia son revisados por personal de tecnología por su incontable número de eventos generados diariamente.

Un evento importante que llegase a pasar desapercibido o no revisado puede ocasionar un incidente de seguridad de la información, que a su vez puede generar un alto impacto de disponibilidad de la información.

En la actualidad la Armada Nacional cuenta con las siguientes herramientas en materia de seguridad de la información:

- Firewall.
- IPS.
- IDS.
- Syslog.
- Analizador de tráfico de la Red.
- DLP.
- Política de Seguridad de la Información.

7.2 MARCO DE REFERENCIA

La Armada Nacional de Colombia, constitucionalmente contribuye a la defensa de la nación. Una de sus funciones es la protección de los medios tecnológicos: informáticos y de comunicaciones, con el cual realiza intercambios de flujos de información de manera efectiva y constante con infraestructuras críticas asignadas por el comando conjunto cibernético del Comando General de las Fuerzas Militares.

Proteger la información es una de sus prioridades, toda vez que por medios electrónicos se envía información clasificada y su objetivo principal es garantizar la integridad, disponibilidad y confidencialidad de la información.

Con la expedición del documento CONPES 3701 y la creación del Comando Conjunto Cibernético de las Fuerzas Militares se planteó la necesidad para cada una de las Fuerzas Militares, crear una dependencia de carácter supervisor mediante la cual se monitoree, revise, prevenga y contrarreste todo tipo de amenazas y/o vulnerabilidades externas que puedan atentar contra la integridad, confidencialidad y disponibilidad de la información.

7.3 MARCO TEÓRICO CONCEPTUAL

La seguridad de la información es sin lugar a dudas un factor indispensable en la vida cotidiana, no solo de las empresas sino de las mismas personas, que día a día se ven comprometidas en materia de seguridad ante los avances tecnológicos y sus inminentes amenazas.

Toda información de cualquier tipo es valiosa para su propietario, y por esto surge la necesidad de protegerla ante peligros potenciales.

Proteger y servir ya no es solo el slogan de un departamento de policía. Actualmente la información debe estar siempre disponible, no alterada y salvaguardada de una manera segura.

Un SIEM (*Security Information and Event Management System*) es una herramienta con la capacidad de monitorear el estado en materia de seguridad de la información de una plataforma tecnológica integrada, con el fin de dar mayor claridad en su comportamiento en aras de prevenir y contribuir a la elaboración de mejores prácticas relacionadas en materia de seguridad.

8. CRONOGRAMA DE ACTIVIDADES

Este proyecto se desarrollará en 5 meses conforme al cronograma presentado en la figura 1, el cual fue acordado con representantes del Comando de la Armada Nacional de Colombia.

Figura 1. Cronograma

Universidad Piloto de Colombia UN ESPACIO PARA LA EVOLUCIÓN		COMANDO DE LA ARMADA NACIONAL DE COLOMBIA											
NOMBRE DEL PROYECTO		IMPLEMENTACIÓN DE UN SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) EN EL COMANDO DE LA ARMADA NACIONAL											
DURACIÓN DE LA EJECUCIÓN DEL PROYECTO EN MESES		5 MESES											
N°	ACTIVIDAD	1	2	3	4	5	6	7	8	9	10	11	12
1	FASE DE DESCUBRIMIENTO												
2	DISEÑO DE RED												
3	LISTADO DE COMPONENTES												
4	SITES SUBREDES												
5	ANALISIS												
6	DEFINIR ALCANCE												
7	FASE DE IMPLEMENTACION												
8	FASE DE PRUEBAS												
9	FASE DE DOCUMENTACIÓN												

Fuente: Los autores, 2016.

Para una efectiva implementación del SIEM, se debe tener en cuenta las siguientes características de diseño, con el fin de asegurar que se cumpla a satisfacción todo el proceso de instalación adecuado.

8.1 FASE DE DESCUBRIMIENTO

Diseño de red: dentro de esta fase se conoce y se revisa el diseño de la red, se requiere información de diagramas de red con el fin de conocer los componentes de seguridad.

Listado de componentes y/o activos: corresponde al listado de aplicativos, motores de bases de datos, dispositivos de red, servidores, personal, listado detallado de direccionamiento y nombres de equipos con su rol o función dentro de la compañía.

Sites, subredes: listado de sitios o subredes.

8.2 DISEÑO Y ANÁLISIS

Definir el alcance de la solución por capas.

- Usuarios.
- Servicios y/o aplicaciones.
- Bases de datos.
- Servidores.
- Dispositivos de red (*routers, switch*).
- Controles de seguridad (IDS, IPS, Firewalls).

8.3 FASE DE IMPLEMENTACIÓN

-
- Definición de recursos.
- Acceso a orígenes de datos.
- Instalación y despliegue.
- Parametrización.
- Configuración de Alertas.
- Correlación.
- Reportes.

8.4 FASE DE PRUEBAS

Durante esta fase se define una serie de pruebas con el fin de verificar y evaluar el funcionamiento de acuerdo al alcance.

8.5 FASE DE DOCUMENTACIÓN

Se documenta todo el proceso, mediante documentos como manuales de operación, manual de instalación, memorias técnicas o posibles mejoras.

9. **PRESUPUESTO**

La elaboración del presupuesto es un valor estimado de los costos en los cuales incurriría la Armada Nacional de Colombia para la implementación de este Proyecto, se presenta en el cuadro 1.

Cuadro 1. Presupuesto

Presupuesto Implementación SIEM					
Fase	**Producto**	**Cant.**	**Descripción**	**Precio Unitario**	**Precio Total**
Descubrimiento	Mano de Obra	8	Obtener Diseño de red	18.000	144.000
	Mano de Obra	24	Obtener Listado de componentes y/o activos	18.000	432.000
	Mano de Obra	4	Obtener información de sites y subredes	18.000	72.000
	Equipo portátil	1	1 equipo portátil	3.000.000	3.000.000
Diseño y Análisis	Mano de Obra	80	Definir alcance y arquitectura de la solución	18.000	1.440.000
	Mano de Obra	120	Integración con componentes	18.000	2.160.000
	Mano de Obra	40	Asesorías	18.000	720.000
Implementación	Mano de Obra	3	Definir método de implementación	18.000	54.000
	Mano de Obra	16	Instalación y despliegue	18.000	288.000
	Mano de Obra	24	Parametrización	18.000	432.000
	Mano de Obra	16	Configuración	18.000	288.000
	Mano de Obra	6	Verificación de alertas	18.000	108.000
	Equipo o MV	1	Equipo de cómputo, MV o capacidad computacional.	8.000.000	8.000.000
	Hosting	1	Hosting (incluye capacidad energética, recursos de red anual)	800.000	800.000
Pruebas	Mano de Obra	40	Elaboración de plan de pruebas y test	18.000	720.000
Documentación	Mano de Obra	40	Elaboración de manuales y memorias técnicas	16.000	640.000
	DVD	3	Material de entrega al cliente DVD	11.000	33.000
	1 resma de Papel	1	Material de entrega al cliente (Documento físico)	14.000	14.000
	Mano de obra	8	Entrenamiento o capacitación	20.800	166.400
Otros		150	Transportes (150 días por 3 personas)	9.000	1.350.000
		5	Servicios (incluye luz, teléfono, internet)	150.000	750.000
		1	Varios – imprevistos	2.000.000	2.000.000
		1	Mobiliarios, recursos de oficina	350.000	350.000
				SUBTOTAL	**23.961.400**
				IVA	**3.833.824**
				TOTAL	**27.795.224**

Fuente: Los autores, 2016.

10. LEVANTAMIENTO TEÓRICO

10.1 ¿QUE ES SIEM?

Hoy en día se están desarrollando nuevas aplicaciones que permiten centralizar el almacenamiento y la interpretación de eventos (desde diversas bitácoras/logs) que provienen de los diferentes sistemas en uso dentro de una organización. Dichas aplicaciones se denominan SIEM[3], del inglés Security Information and Event Manager. Ahora bien, se hace necesario realizar algunas consideraciones previas respecto de la terminología y los acrónimos que se emplean en esta área. Si bien las siglas SEM, SIM y SIEM que será la que emplearemos en este trabajo se han utilizado como equivalentes, aluden a sistemas con diferentes características y capacidades:

SIM (Security Information Management): hasta hace un par de años, esta sigla era la que predominaba haciendo referencia al almacenamiento de datos durante largo plazo (logs, eventos, etc.) así como al análisis y reporte de los datos registrados.

SEM (Security Event Management): este tipo de gestión es relativamente novedosa. Se utilizan estos sistemas para monitorear en tiempo real y correlacionar diversos eventos, posibilitan generar notificaciones y obtener reportes.

SIEM (Security Information Event Management): este tipo de sistemas permite obtener, analizar y presentar información obtenida de diversos dispositivos y aplicaciones. Cuentan con herramientas de administración y manipulación de políticas, permiten auditar diversos tipos de sucesos, filtrar datos para investigar incidentes y monitorear la utilización de privilegios.

En este tipo de sistemas, las características mencionadas permiten dar soporte y efectividad a las tareas de seguridad en el ámbito de la infraestructura computacional de la organización.

Estos sistemas poseen, en síntesis, las siguientes capacidades:

- Recolección de datos y eventos.
- Agregación y correlación de los mismos en tiempo real.[4]
- Interfaces hombre-máquina adecuada para visualizar, monitorear y administrar los eventos.

3 MILLER, D; Harris, S; HARPER, A; VANDYKE, S & BLASK, C. Security Information and Event Management. (SIEM) Information, Network Pro Library 1 st, ed, 2010.

4 CUPPENS, Frederic; AUTREL, Fabien; MIEGE, Alexandre; BENFERHAT, Salem; and EGE, Re Mi. Correlation in an intrusion detection process, 2002.

- Respuesta automática para aquellos eventos que tienen relación directa con la seguridad.

Por otra parte, los sistemas SIM se caracterizan principalmente por permitir mayor análisis histórico de los datos y eventos almacenados en los mismos. Así como también incluyen la posibilidad generar diversos tipos de reportes. Estos sistemas posibilitan también el aplicar técnicas de correlación sobre los datos y eventos, pero no en tiempo real. Se cuenta en ellos con un repositorio para los sucesos (logs) y, por lo general, algún mecanismo flexible de consulta que permite obtener reportes diversos.

En ambos tipos de sistemas, se dispone de la posibilidad de aplicar filtros, ya que es común hoy en día la gran cantidad de datos que se obtienen, generan y almacenan, por la naturaleza propia de las actividades de los mismos, entre ellos: Intrusión Detección System (IDS), firewalls, logs de aplicaciones.

10.2 CARACTERIZACIÓN DE SISTEMAS SIEM

Ahora bien, como una instancia mejorada y ampliada, los sistemas SIEM se caracterizan por combinar las características de los sistemas de tipo SEM y SIM, de ahí el acrónico que los representa actualmente.

Una de las principales características, entonces, es que estos sistemas poseen tecnologías adecuadas para correlacionar diversos tipos de datos de diversas fuentes de origen. La posibilidad de contar con una correlación es aquella capacidad de establecer y formar relaciones entre los diversos datos (logs, sucesos, etc.) de diferentes dispositivos (ya sean de software o hardware). Dichas correlaciones se basan en características tales como: origen, destino, protocolo o tipo de evento. Además, las correlaciones en sí mismas permiten filtrar información duplicada y/o redundante para así poder eliminar aquellos sucesos que entorpecen un análisis adecuado. De esta manera, los administradores de la infraestructura de la organización pueden manipular mayor cantidad de sucesos más rápidamente, con mayor efectividad, haciendo uso de información correcta y suficiente para así poder encarar acciones adecuadas y establecer nuevas políticas a futuro (según el tipo de suceso).

Cabe destacar que las correlaciones se establecen, básicamente, mediante dos mecanismos de análisis de los datos: mediante reglas preestablecidas (que analizan los patrones de los sucesos) o bien en base al análisis estadístico de los mismos. Y, por supuesto, al establecer correlaciones se debe tener en cuenta el periodo de ocurrencia de los sucesos. El tiempo en este tipo de sistemas es un factor fundamental para el análisis y las acciones subsiguientes que se deberán tomar. Las características más específicas de los SIEM pueden sintetizarse de la siguiente manera:

- Agregación de datos: cuentan con la posibilidad de adquirir información de diversas fuentes: redes, servidores, bases de datos, aplicaciones, etc. Con la capacidad para consolidar los datos obtenidos y no perder sucesos importantes.

- Correlación: a través de diferentes mecanismos, se efectúa una búsqueda sobre atributos comunes y se establecen relaciones entre diversos sucesos, para poder unirlos y verlos como un único evento, aunque los datos provengan de diferentes fuentes.

- Alertas: análisis automático y generación de alertas para notificar a los administradores de los sucesos más relevantes.

- Capacidad forense: la posibilidad de utilizar herramientas de investigación y análisis para poder explorar las alertas, determinar el origen de los sucesos y así organizar las acciones preventivas.

- Tablero de instrumentos: estas herramientas toman los datos de los distintos sucesos y posibilitan visualizarlos a través de diferentes mecanismos gráficos, adecuados para la interacción de los usuarios del sistema, de tal forma que estos puedan identificar a simple vista patrones diversos de funcionamiento del sistema y alertas recientes.

- Cumplimiento: son utilizadas para automatizar la recolección de datos que satisfacen los requisitos/políticas de seguridad para la organización. Gracias a ellos, se pueden producir reportes que se adapten a los procesos de auditoria internos.

- Archivo: estos sistemas permiten almacenar por largo tiempo un gran volumen de datos para facilitar luego las tareas de correlación propias de los mismos durante su tiempo de vida.

10.3 IMPORTANCIA DE UN SIEM

Para mejorar la capacidad de identificar una actividad inapropiada o inusual, las organizaciones pueden integrar el análisis de la información con análisis de vulnerabilidades, los datos de rendimiento, monitoreo de red y el registro de auditoría del sistema (log), esta información se logra a través del uso de herramientas SIEM. Las herramientas SIEM son un tipo de software de registro centralizado que puede facilitar la agregación y consolidación de los registros de múltiples componentes del sistema de información. Las herramientas SIEM también pueden facilitar la auditoría de correlación de registros y análisis. La correlación de la información de registro de auditoría con la información de análisis de vulnerabilidades es importante para determinar la veracidad de los análisis de

vulnerabilidad y correlacionar eventos de detección de ataques con resultados de la exploración.

Los productos SIEM generalmente incluyen soporte para muchos tipos de orígenes de registros de auditoría, tales como sistemas operativos, servidores de aplicaciones (por ejemplo, servidores web, servidores de correo electrónico), y software de seguridad, e incluso pueden incluir soporte para dispositivos de control de seguridad física, tales como lectores de tarjetas.

Un servidor SIEM analiza los datos de los diferentes orígenes de registros de auditoría, correlaciona eventos entre las entradas de registro de auditoría, identifica y prioriza los eventos importantes, y se puede configurar para iniciar las respuestas a los acontecimientos. Para cada tipo de origen de registros de auditoría, los productos SIEM normalmente se pueden configurar para proporcionar la funcionalidad de categorizar los campos de registro de auditoría más importantes que puede mejorar significativamente la normalización, análisis y correlación de datos de registro de auditoría.

El software SIEM también puede realizar la reducción de eventos al prescindir de los campos de datos que no son importantes para la seguridad del sistema de información, que podría reducir el ancho de banda de la red y los datos de uso del almacenamiento del software SIEM.

11. CONTEXTUALIZACIÓN DEL ENTORNO

11.1 CRITERIOS

Los criterios establecidos por la Armada para la ejecución del presente proyecto son:

11.1.1 Software libre. La Armada tendrá la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el producto de software en cualquier sistema de computación, cumpliendo a cabalidad con las normas de derechos de autor sobre el software instalado.

11.1.2 Software Gratuito. Que sea un tipo de software que se distribuya sin costo, disponible para su uso, por tiempo ilimitado, que permita su redistribución, pero con algunas restricciones, como no modificar la aplicación en sí, ni venderla, y dar cuenta de su autor.

11.1.3 Comunidades, foros de discusión y consultas. Al establecer como primer criterio que la solución sea Software Libre y gratuito, es necesario indicar que se debe contar con un portal o páginas web que permitan acceder a la documentación, procesos de instalación, foros y comunidades que permitan su consulta.

11.1.4 Plataformas. Se recomienda que la solución opere bajo plataformas basadas en distribuciones *UNIX o LINUX*, teniendo en cuenta el mismo concepto de software libre.

11.1.5 Escalabilidad. El sistema debe tener la propiedad de adaptarse al crecimiento continuo sin perder la calidad en los servicios, permitiendo tanto escalabilidad vertical como escalabilidad horizontal.

11.1.6 Capacidad de integración con la Infraestructura dispuesta. El sistema debe estar en la capacidad de integrarse con la infraestructura disponible y la que se designe vincular en común acuerdo, sin la necesidad de adquirir productos adicionales utilizando los protocolos estándares en el mercado.

11.1.7 Cumplimiento con los acuerdos de confidencialidad. La Armada pone a disposición los formatos establecidos en el sistema de gestión de calidad, los cuales deberán ser diligenciados por el personal que ejecutará el proyecto.

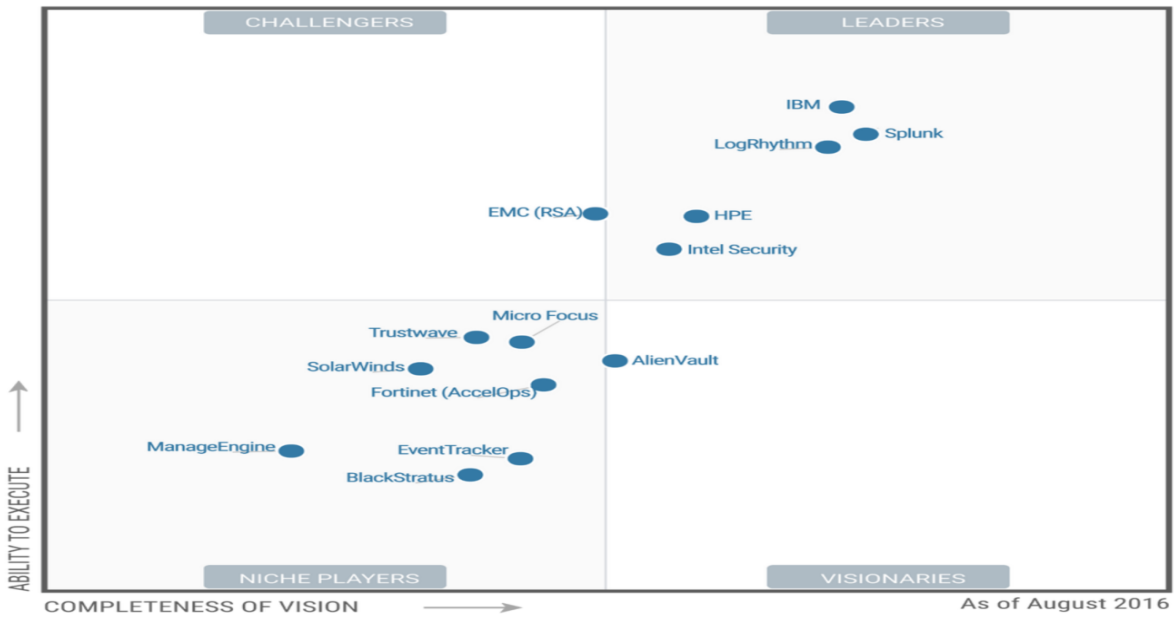
11.1.8 Experiencia. Con el fin de generar confiabilidad en la herramienta, esta deberá contar por lo menos con 3 años de experiencia en el mercado y en lo posible con casos de uso de implementación en Colombia.

11.2 ANÁLISIS

Dentro de las fuentes de información, se tiene en cuenta el cuadrante mágico de *Gartner* figura 2, proveniente de la empresa *Gartner Inc*., la cual es una empresa de consultoría dedicada a la investigación de las industrias de Tecnologías de la Información (TI), analizando las tendencias en el mercado que facilitan la selección de soluciones y productos tecnológicos, mediante un esquema propio de trabajo que provee gráficamente el posicionamiento de tecnología en los ejes X(visión) Y(habilidad de ejecución).

Para el presente proyecto se toma el caso de investigación referente al cuadrante mágico para (SIEM) *Security Information and Event Management*, donde se relacionan los fabricantes de este tipo de tecnologías y su representación o posicionamiento dentro del cuadrante, publicado en agosto de 2016:

Figura 2. Cuadrante mágico de *Gartner SIEM* 2016



Fuente: http://www.gartner.com.

Así mismo, teniendo en cuenta los criterios y casos de uso, se investiga soluciones de software libre utilizadas en entidades estatales y privadas que permitan recoger las experiencias en su funcionamiento y su implementación, se encontraron entre ellas:

Empresa de Telecomunicaciones de Bogotá – ETB: utiliza un sistema basado en componentes libres tales como *Logstash, Elasticsearch, Kibana y Plugins* de análisis y visualización de estados y reportes.

Mozdef: documentado en http://mozdef.readthedocs.org/en/latest/overview.html utiliza básicamente los mismos componentes que son utilizados por ETB, incluyendo el *plugin de Mozdef* y otros componentes que robustecen la solución.

Prelude: documentado en http://www.prelude-siem.com/.

En el cuadro 2, se verifican cada una de estas soluciones, identificando aquellas que cumplan con los criterios de software libre inicialmente propuestos para el desarrollo del presente proyecto, obteniendo el siguiente resultado:

Cuadro 2. Comparativo Software Libre

Solución	Fuente De Información	Observaciones	Aplica/No Aplica
IBM	https://www-112.ibm.com/software/howtobuy/buyingtools/paexpress/Express?P0=E1&part_number=D0WR5LL,D0WR8LL,D0WRBLL,D0WRELL,D0WRHLL,D0WRKLL,D0WRNLL,D0WRRLL,D0WRULL,D0WSCLL,D0WSFLL,D0WSILL,D0WSLLL,D0WSPLL,D0WSSLL,D0WSVLL,D0WSYLL,D0WRXLL,D10U8LL,D10UDLL,D10UGLL,D10UKLL,D10UVLL,D1140LL,D121DLL,D121FLL,D121ILL,D121KLL,D121MLL,D121PLL,D121RLL,D121TLL,D121CLL,D1227LL,D1229LL,D122BLL,D122DLL,D122ELL,D122HLL,D122ILL,D122KLL,D122MLL,D122PLL,D123GLL,D123ILL,D123KLL,D123LLL,D124KLL,D1BXELL,D1BXCLL,D1BWGLL,D1BWELL,D1BWKLL,D1BWILL,D1BWWLL,D1BWULL,D1BWQLL,D1BXILL,D1BXGLL,D1BWSLL&catalogLocale=es_ES&Locale=es_ES&country=ESP&PT=jsp&CC=ESP&VP=&TACTICS=&S_TACT=&S_CMP=&brand=SSNP22	En la página web del fabricante indica los precios del producto SIEM de IBM denominado QRADAR en donde se indica un valor asociado al licenciamiento del producto.	No Aplica
HP	http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/try-now.html	En la página web del fabricante indica que el producto cuenta con un trial por 30 días.	No Aplica

Cuadro 2. (Continuación)

Solución	Fuente de Información	Observaciones	Aplica/No aplica
Blackstratus	http://www.blackstratus.com/download-log-storm-form/	En la página web del fabricante indica que el producto cuenta con un periodo de evaluación de 14 días	No Aplica
Splunk	http://www.splunk.com/en_us/products/splunk-enterprise/free-vs-enterprise.html	En la página web del fabricante indica que cuenta con tres tipos de producto entre ellos Splunk Free.	Si Aplica
Intel security	http://www.mcafee.com/us/products/siem/index.aspx	En la página web cuenta con una versión trial limitada de descarga.	No Aplica
LogRhythm	https://logrhythm.com/products/siem/	En la página web cuenta con chat on line, en donde se realizó la consulta e indican que ofrecen un Demo, utilizado para demostración del producto.	No Aplica
EMC(RSA)	http://colombia.emc.com/support/rsa/eops/siem.htm	En la página web cuenta con chat on line, en donde se realizó la consulta e indican que ofrecen un costo asociado al mantenimiento del sistema que se ofrece en términos anuales.	No Aplica
SolarWinds	http://www.solarwinds.com/siem-security-information-event-management-software.aspx	En la página web del fabricante indica que el producto cuenta un periodo de 30 días con todas las funcionalidades y su precio empieza 4495 dólares.	No Aplica
TrustWave	https://www.trustwave.com/Products/SIEM/	Se realiza contacto vía e-mail, indicando que el producto cuenta con costos asociados al soporte del producto que permiten mantener sus actualizaciones y soporte directo.	No Aplica
MicroFocus	https://www.netiq.com/products/sentinel/how-to-buy/	En la página web del fabricante indica que cuenta con una versión Trial y un link asociado donde indica cómo comprar el producto.	No Aplica
AlientVault	https://www.alienvault.com/products/ossim	En la página web del fabricante indica que dentro de los productos ofrecidos cuenta con OSSIM (open source)	Si aplica
EventTracker	https://www.eventtracker.com/pricing/comparison/	Se requiere suscripción anual por las soluciones que ofrece.	No Aplica
AccelOps	http://www.accelops.com/free-trial/	El producto cuenta con una versión trial por 30 días	No Aplica
Mozdef	http://mozdef.readthedocs.org/en/latest/overview.html	Utiliza componentes de software libre tales como kibana, logstash, elasticsearch.	Si Aplica
Solución	Fuente de Información	Observaciones	Aplica/No aplica
Prelude	http://www.prelude-siem.com/index.php/uk/products/overview http://www.prelude-siem.com/en/home-page-2/products/choose-your-version/	En la página web del fabricante indica que cuenta con tres tipos de producto entre ellos Prelude OSS basado en licenciamiento GPlv2.	Si Aplica

Fuente: Los autores, 2016.

En el cuadro 2 se identifica la solución o marca del SIEM, la referencia de la información o vínculo de la página web donde se encuentra el detalle del mismo,

en las observaciones se describe algunas limitantes del producto impuestos por el fabricante que no aplican de acuerdo a lo solicitado dentro de los requerimientos iniciales de la Armada Nacional y basados en estas premisas se indica en la última columna Si Aplica o No Aplica para tener en cuenta dentro de la selección de las soluciones SIEM a evaluar.

Por lo anterior dentro de las soluciones evaluadas que cumplen los primeros criterios de software libre se encuentran:

- ***SPLUNK.***
- ***OSSIM (ALIENT VAULT).***
- ***MOZDEF.***
- ***PRELUDE (OSS).***

Teniendo en cuenta los criterios establecidos, se analizarán cada una de estas soluciones, de acuerdo a sus características, ventajas y desventajas:

11.2.1 Splunk

Página web: http://www.splunk.com/.
Foros o comunidad: http://www.splunk.com/en_us/community.html.
Documentación técnica: http://docs.splunk.com/Documentation.
Plataformas: *Unix, Linux, Windows, Solaris, MAC OS.*

Descripción: Software de búsqueda, monitoreo y análisis de datos generados por equipos *Big Data* (figura 3).

Figura 3. Logo Splunk

Fuente: www.splunk.com.

Ventajas:

- Confiabilidad en el producto, al encontrarse en el cuadrante mágico de *Gartner*.
- *Dashboards* (paneles visuales) personalizables.
- Búsqueda en tiempo real.

Desventajas:

- Puede indexar solo hasta 500 MB por día.
- Balanceo de carga no *cluster.*
- *Analytics.*

11.2.2 Alient Vault OSSIM.

Página web: https://www.alienvault.com/products/ossim.
Foros o comunidad: https://www.alienvault.com/forums/.
Documentación técnica: https://www.alienvault.com/documentation.
Plataformas: Propietaria basada en Linux.

Descripción: Producto que contiene tres componentes, USM Sensor que se encarga de colectar los logs y tráfico de red. USM Server acepta y correlaciona la información que trae el sensor y USM Logger que asegura los eventos en formatos tipo RAW (figura 4).

Figura 4. Logo *Alient Vault OSSIM*.

Fuente: www.alientvault.com.

Ventajas:

- Confiabilidad al encontrarse en el cuadrante mágico de Gartner.
- Búsqueda en tiempo real.

Desventajas:

- Permite implementar en un solo servidor.
- Permite únicamente tres niveles de plantillas para los reportes.
- La retención de logs se aplica únicamente para eventos.
- Los componentes se administran individualmente.
- Permite únicamente un usuario para la administración.
- Recolección de logs limitado.

11.2.3 Mozdef

Página web: http://mozdef.readthedocs.org/en/latest/overview.html.
https://www.elastic.co/.
Foros o comunidad: https://www.elastic.co/community.
Documentación técnica: https://www.elastic.co/guide/index.html.
Experiencia y casos de uso: https://www.elastic.co/use-cases.
Plataformas: *Unix, Linux, Windows.*

Descripción: Utiliza tres componentes básicos, *Logstash* que recoge, normaliza y transporta los datos, *elasticsearch*, que distribuye escalablemente, indexa y busca los datos y *kibana* que es la plataforma de análisis, graficación y sumarización de los datos. El *plugin* de *Mozdef* utiliza estos recursos y permite incluir un trabajo colaborativo en los incidentes de seguridad agregando métricas, alertas y geolocalización (figura 5).

Figura 5. Logo Mozdef

Fuente: https://mozdef.readthedocs.io.

Ventajas:

- Confiabilidad al encontrar caso de uso a nivel nacional.
- Escalabilidad horizontal, permite crear múltiples instancias y nodos bajo un *cluster* que indexa la información tomando ventaja de hardware adicional.
- Cuenta con un gran motor de Búsqueda con funciones como multilenguaje, geolocalización, autocompletar.
- Orientado a documento, utiliza un esquema libre basado en documentos *JSON* estructurados indexando todos los campos por defecto.
- Persistencia, registro de transacciones en los nodos del *cluster* para minimizar pérdida de datos.
- Opera bajo licencia libre.
- Crea mapas, histogramas, gráficos circulares, barras, tendencias.
- Interfaz fácil de usar, para crear, guardar y compartir visualización de datos.
- Cuenta con 200 complementos que ayudan a procesar logs y eventos de gran variedad de sistemas y fuentes de datos.
- Integra administración de incidentes.
- Balanceo de carga *(cluster).*

Desventajas:

- El componente de *Kibana* no permite utilizar múltiples niveles o roles de usuarios.

11.2.4 Prelude OSS.

Página web: http://www.prelude-siem.com/index.php/uk/.
Foros o comunidad: http://www.prelude-siem.com/index.php/uk/community.
Documentación técnica: http://www.prelude-siem.com/index.php/uk/community/documentation.
Casos de uso: http://www.prelude-siem.com/index.php/uk/customer/references.

Descripción: compuesto por *Prelude- correlator* y *prelude LML* para el análisis de registros, los eventos los maneja a través de (IDMEF – *Intrusion Detection Message Exchange Format*), (figura 6).

Figura 6. Logo Prelude

Fuente: www.prelude-siem.com.

Ventajas:

- Arquitectura modular distribuible y disponible en componentes.
- Interfaz fácil de usar, para crear, guardar y compartir visualización de datos.
- Cuenta con complementos para ayudar a procesar los logs y eventos de diferentes fuentes de datos.
- Integra administración de incidentes.
- Opera bajo licencia libre.

Desventajas:

- Almacena alertas únicamente.
- Mono servidor.

11.3 TABLA COMPARATIVA DE LOS PRODUCTOS

En la tabla 1, se presentan los resultados generados del anterior análisis con las soluciones SIEM, identificando las características significativas solicitadas por la Armada.

Tabla 1. Tabla comparativa productos SIEM

Descripción	*Splunk*	*Alient Vault OSSIM*	*Elastic Mozdef*	*Prelude*
Basado en software libre	Si	Si	Si	Si
Escalabilidad horizontal	No	No	Si	No
Capacidad de almacenamiento y procesamiento de *logs*.	Limitada	Limitada	De acuerdo a hardware	De acuerdo a Hardware
Posibilidad de transferencia segura de datos.	Si	Si	Si	Si
Visualizaciones de estado diario, semanal, anual.	Si	Si	Si	Si
Gestor de Incidentes	No	No	Si	Si
Normalización de eventos.	Si	Si	Si	Si
Cluster o balanceo de carga	Si	Si	Si	No
Dashboard personalizables	Si	Si	Si	Si
Experiencia				
Casos de uso, acercamiento clientes conocidos	Si	Si	Si	No
Experiencia en el mercado	12 años	9 años	7 años	10 años
Soporte y documentación				
Cuenta con sitio web de foros y comunidad para soporte	Si	Si	Si	Si
Calificación	100	100	120	90

Fuente: Los autores, 2016.

Teniendo en cuenta el resultado obtenido con mayor calificación, se determina como solución la implementación de la herramienta *MOZDEF* la cual incluye tres componentes dentro de su infraestructura *ELASTIC SEARCH, LOGSTASH Y KIBANA.*

11.4 DOCUMENTACIÓN DE LA INFRAESTRUCTURA

11.4.1. Topología de Red. Al presente documento se adjuntó el Diagrama de red de la Armada (*Anexo A. Diagrama de red de la Armada Nacional*) en donde se identifica los componentes de infraestructura.

11.4.1.1 Red Integrada de Comunicaciones RIC. La Red Integrada de Comunicaciones RIC, es el activo más valioso y de mayor importancia del Sector Defensa, la Fuerza Pública y en especial del Comando General de las Fuerzas Militares, para el Comando y Control de las operaciones que adelantan cada una de las Fuerzas en cumplimiento de su misión y las que realizan conjuntamente[5].
Tiene como función garantizar los servicios de comunicaciones y sistemas de información a nivel estratégico nacional con efectividad y oportunidad para la defensa, soberanía, independencia e integridad del territorio nacional.

Para ello la Jefatura Control de Comunicaciones y Sistemas, cuenta con una red estratégica de transmisión terrestre con cobertura nacional, conformada por enlaces de alta capacidad, la cual se comporta como la columna vertebral para la prestación de servicios a lo largo y ancho del territorio nacional.
En la realización de las operaciones, dependiendo del terreno y dada la extensión territorial, provee a los comandantes los canales de comunicaciones con sus unidades subalternas, tanto en sus sedes habituales como en su área de responsabilidad.

11.4.1.2 Características de la RIC. La Red Integrada de Comunicaciones acorde con sus capacidades cuenta con las siguientes características:

11.4.1.3 Cobertura. La Cobertura de la Red Integrada de Comunicaciones del Comando General de las Fuerzas Militares, apoya el ejercicio de mando y control en todos sus niveles empleando tecnologías de punta para la transmisión de voz, datos y video en todo el territorio nacional a través de sus centrales de microondas, terminales y sitios de repetición que se encuentran conectadas al centro de datos de la Red Integrada de Comunicaciones (RIC), contando con una plataforma tecnológica acorde con las necesidades de las Fuerzas.

Las Fuerzas Militares de Colombia, se apoyan en los servicios que ofrece la Red Integrada de Comunicaciones, facilitando la planeación y ejecución de las Operaciones Militares, Conjuntas y Coordinadas.

11.4.1.4 Seguridad. La Red Integrada de Comunicaciones cuenta con protocolos de seguridad en instalaciones físicas, transmisión de voz y datos, que garantiza la integridad y confidencialidad de la información estratégica en el sector defensa.

5 COMANDO GENERAL FFMM. Manual uso Red Integrada de Comunicaciones CGFM, 2015, versión 1.

11.4.1.5 Disponibilidad. Permite mantener los sistemas de la RIC para ser utilizados como apoyo a las operaciones conjuntas coordinadas e inter agénciales en el momento que sean requeridas. Esta estrategia tecnológica pretende garantizar que las herramientas tecnológicas estén disponibles 24 (horas) x 7 (días) X 12 (meses) para las unidades militares, sin importar su despliegue y ubicación, permitiendo optimizar las capacidades de acción y reacción.

11.4.1.6 Proveedor de Servicios de Internet (ISP). La Armada Nacional anualmente contrata servicios de entidades prestadoras de servicios de internet con el fin de transportar datos e internet a las unidades de la Armada Nacional como medio alterno a la RIC.

11.4.2 Aplicaciones. Actualmente el portafolio de aplicaciones de la Armada Nacional de Colombia está constituido por los siguientes sistemas misionales y de apoyo.

11.4.2.1 Misionales

- **Sistema SIGO – Sistema de Información Geográfico Operacional.** Cargue y visualización de resultados operacionales y situación de las unidades de la Armada Nacional.
  Tipo de Desarrollo: Desarrollo a la medida.
  Número de Usuarios: 30 usuarios nivel nacional Armada (Fuerzas-Brigadas-Batallones, COIC, JINA).
  Interpretación de la Información: Estadísticas de DIONA, Guardia COA, BISIGOI del COIC, CAPRICORNIO y SINAVALE.
  Seguridad: Usuario-contraseña, restricción por IP, uso de TOKENS Sistema de Información Geográfico Operacional Conjunto – SIGOC.

- **Sistema de Información Administración del Talento Humano (SIATH).** Es el sistema de información que permite el registro y administración de las hojas de vida de los funcionarios civiles y militares del sector defensa, así como la gestión de los procesos de prestaciones sociales.

- **Sistema de Información Jurídico (SIJUR).** Es una aplicación que permite unificar los procesos disciplinarios para personal civil y para el personal militar, procesos administrativos tanto para personal civil y militar y procesos penales para personal uniformado del sector defensa.

- **Sinergia Logística (SILOG).** Es la implementación del ERP SAP R/3 que brinda a las diferentes entidades pertenecientes al Ministerio de Defensa la posibilidad de llevar el control de los procesos logísticos, financieros, de mantenimiento y de sanidad del sector defensa.

- **Sistema de información geoestratégico CAPRICORNIO.** Sistema de Información para la georeferenciación de resultados operacionales, unidades y todos los servicios en aspectos georeferenciales.
  Usuario Principal: JONA - DIONA.
  Tipo de Desarrollo: Desarrollo a la medida donado por el Departamento de Defensa de los Estados Unidos.
  Número de Usuarios: 30 usuarios a nivel nacional Armada (Fuerzas-Brigadas-Batallones, COIC, JINA).
  Insumo de la Información: Base de datos del SIGO, Cartografías del: Agustín Codazzi, EJC, FAC, DIMAR.
  Seguridad: Usuario-contraseña, restricción por IP, uso de TOKENS.

- **Portal Web** www.armada.mil.co. El portal WEB de la Armada Nacional ofrece al usuario de forma fácil e integrada, el acceso a una serie de recursos y servicios relacionados a un mismo tema, Incluye: enlaces, buscadores, foros, documentos, aplicaciones, compra electrónica, etc. Está dirigido a resolver necesidades de información específica y registrar los casos de quejas y reclamos de la población civil.

- **Intranet marinanet.armada.mil.co.** En la Intranet de la Armada Nacional se ofrece al usuario interno y externo de forma fácil e integrada, el acceso a una serie de recursos y servicios relacionados a un mismo tema. Incluye: enlaces, órdenes del día, enlaces con escuelas, certificados de haberes, etc. Está dirigido a resolver necesidades de información específica.

- **Correo Electrónico institucional.** Este sistema ofrece servicios de mensajería a la Armada Nacional. Se encuentra habilitado el servicio de OWA para los funcionarios autorizados de acuerdo a formato y directiva de políticas de seguridad y para todos los agregados militares. Así mismo para las unidades externas de la ARC.

11.4.2.2 De Apoyo

- **Sistema de Gestión Documental ORFEO.** Es un sistema de Gestión Documental con licencia GPL que permite la gestión y administración de documentos generados por el Comando General especialmente la información para las vigencias 2006 al 2013 y parte del 2014 de todos los procesos de contratación. Este sistema permite la digitalización de la información y posterior consulta para todos los funcionarios de dicha oficina.

- **Suite Visión Empresarial.** Este sistema es una aplicación integral que facilita la toma de decisiones y mantiene actualizado el sistema de gestión de calidad (mapa de riesgos, plan de acción, indicadores de gestión, procesos

informáticos) y registra la inversión económica, para mantenimiento y gestión de la infraestructura tecnológica.

11.4.3 Plataformas seguridad informática

- **Plataforma.** En la Plataforma de seguridad informática de la Armada se encuentran instalados dos Firewalls en alta disponibilidad en la red perimetral para controlar el acceso a la red de la Armada, red desmilitarizada (DMZ), usuarios de Internet y canales dedicados externos Red de alta velocidad del estado (RAVEC), SIIF, Agencia Logística, CAVIM y dos *Firewall* internos en alta disponibilidad para las conexiones con red Administrativa, granja de Servidores, unidades remotas. Las conexiones remotas de esta red están además aseguradas con redes privadas virtuales *VPN(s).*

- **Consola de Antivirus.** El servicio de antivirus tiene la funcionalidad de detectar y eliminar virus informáticos, *malware*, troyanos, *rootkits*. Cuenta además con rutinas de detención, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema, bloqueo de memorias *USB* y puertos específicos.

- **Sistema de Control de Contenidos.** Controla y/o deniega el acceso a Internet de los usuarios autorizados y permite que los administradores de red controlen o supervisen el tráfico de red a Internet. Adicionalmente trabaja junto con dispositivos de integración (servidores, *proxy, firewalls, routers*) y proporciona las herramientas de configuración y el motor de base de datos necesario para desarrollar, supervisar y aplicar políticas de acceso a Internet.

- **Sistema de Detección y Prevención de Intrusos.** (IPS *Intrusion Prevention System*) es un software que ejerce el control de acceso a la red del ARC para proteger los sistemas computacionales y la plataforma tecnológica de ataques y abusos. Este sistema controla el acceso a la red basado en los contenidos del tráfico, en lugar de direcciones IP o puertos.

  El sistema de prevención de intrusos, al igual que el sistema de detección de intrusos, funciona por medio de módulos, pero la diferencia es que esta última alerta al administrador ante la detección de un posible intruso (usuario que activó algún Sensor), mientras que un sistema de prevención de intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque informático.

- ***Firewall* de aplicaciones *WEB (WAF).*** Se cuenta con dos sistemas para protección de aplicaciones web, uno que protege todos los portales tanto internos como externos (“granja y DMZ”), este en formato *appliance* (“servidor

físico”) y un *WAF* para la protección del correo y la página web en formato *cloud* (“computación en la nube”).

- **Anti Ataques de Denegación de servicio (*DDoS)*.** Se cuenta con un servidor para la protección contra ataque de denegación de servicios instalado en el borde externo de la red.

- **Bases de datos (DBF).** El Sistema de prevención de intrusos a base de datos y por sus siglas DBF *Database Firewall* se encuentra instalado de cara a los servidores de la granja y sobre las bases de datos con el fin de prevenir perdidas de información.

12. DESARROLLO

12.1 ACUERDOS DE CONFIDENCIALIDAD

Teniendo en cuenta que corresponde a un ente del Estado que requiere reserva en la información, es necesario establecer los acuerdos de confidencialidad estipulados dentro de los procesos de gestión de calidad que permitan garantizar a la Armada que el presente proyecto se adecúe con los lineamientos y políticas, por tal razón es necesario el diligenciamiento del formato Acuerdo de Confidencialidad Armada Nacional que forma parte de este documento (Anexo B).

12.2 ESTRATEGIA DE ÉXITO EN LA IMPLEMENTACIÓN

Basándose en los documentos consignados y publicados en la *National Institute of Standards and Technology (NIST)* - Instituto Nacional de Estándares y Tecnología, relacionados con las mejores prácticas recomendadas para la implementación y administración de sistemas *SIEM* se definen los siguientes componentes para cumplir con éxito la gestión de los registros a través de un sistema *SIEM*.

Estrategia de Administración de logs:

- Centralizar todos los eventos de logs relevantes.
- Estos eventos deben ser filtrados, agregados y/o normalizados.
- Definir y documentar el alcance.
- Definir cuáles son las redes protegidas.
- Definir el (ROA) *Record of Authority, document* que define cuáles serán los logs para almacenar y el periodo de retención.
- Definir los eventos de Interés (EOI*) Events of Interest.*
- Definir los reportes visuales.

Informes y revisión:

- Proveer reportes ejecutivos o resumidos.
- Proveer reportes que permitan agruparse por el dueño de la aplicación o por tipo de autenticación.
- Proveer un Top 10 de todos los dispositivos asociados a la infraestructura.
- Agrupar por ID o nombres los equipos finales que detecten *malware.*

Sistema de seguimiento a incidentes.

Para todos los eventos de interés identificados como amenazas en tiempo real, es necesario generar un incidente, con la descripción del problema y la solución y sistema de incidentes con el fin de generar métricas asociadas al sistema.

12.3 DEFINICIÓN DEL ALCANCE

Se establecen (3) tres etapas para definir el alcance del proyecto:

- Definir los activos de Información que se integrarán con el SIEM.
- Definir los Eventos de Interés por parte del cliente.
- Definir los reportes o visualizaciones.

Para la definición del alcance del proyecto se tomaron en cuenta los activos de la Infraestructura Tecnológica dispuestos por la Armada de acuerdo a la calificación del riesgo. Los cuales se encuentran discriminados en el Anexo C.

Inicialmente se tomaron los equipos catalogados como confidencial con una calificación de integridad = 5, confidencialidad = 5 y disponibilidad = 5 es decir considerados como activos críticos dentro de la Armada.

12.3.1 Definición Activos De Información. Al realizar la revisión detallada de la Infraestructura se identificó un equipo recolector de *logs* llamado *analyzer*, el cual almacena la información de eventos de los equipos críticos y permite centralizarlos, este recolector será una de las fuentes iniciales y principales utilizadas para alimentar el SIEM.

Dentro de las reuniones llevadas a cabo en la Armada Nacional de Colombia se determinó que el segundo elemento de la infraestructura para implementar dentro de la solución que cumple con los parámetros de Infraestructura crítica con una calificación de integridad = 5, confidencialidad = 5 y disponibilidad = 5 corresponde a la Infraestructura de correo electrónico, con lo anterior se definen los siguientes elementos:

Analyzer (máquina especializada en recolectar logs de 60 equipos firewall, anti-DoS, IPS, *Web Application Firewall* (WAF) y servidores de página web e intranet que se encuentran en la red de la Armada Nacional de Colombia.
Infraestructura de correo electrónico compuesto por (2) dos servidores uno que compone el SMTP y el otro con el servicio POP y almacenamiento y en su borde un antispam de correo.

12.3.2 Definición activos de información. Se definen los eventos o registros que son de interés y sobre los que se realizarán los filtros.
Analyzer: categoriza los eventos basados en su nivel de criticidad:

- Alta.
- Media.
- Baja.

Infraestructura de correo: categorización de los eventos basados en un equipo *Anti Spam* que filtra los correos maliciosos, inspecciona los adjuntos en busca de virus y genera alertas que son enviadas a un correo del administrador.

Categorización de los eventos basados en su nivel de criticidad:

- Alta.
- Media.
- Baja.

12.3.3 Definición reportes o visualizaciones. Se definen los reportes que son de interés y los cuales se generarán en la plataforma.

Analyzer**:** Permite identificar la visualización de reportes donde se representan:

- Top 10 de ataques realizados en tiempo real.
- Top 10 de direcciones IP fuentes de donde provienen los ataques.
- Mapa o geolocalización que identifique IP fuente.

Infraestructura de correo electrónico: el correo electrónico corre sobre una plataforma *Open Source*, ZIMBRA y servidor *Linux* para poder generar cuentas de correo a todo el personal de la Armada Nacional sin tener que pagar un costo tan alto por licenciamiento.

12.4 DISEÑO

12.4.1 Componentes y arquitecturas SIEM. *Mozdef* está compuesto por (3) tres componentes básicos para su funcionamiento los cuales se visualizan en la figura 7.

Figura 7. Componentes SIEM Mozdef

Fuente: https://www.freebsdnews.com/2016/03/18/elk-first-part/.

Conjuntamente, existen componentes adicionales que incrementan sus funcionalidades y complementan la solución entre ellos se encuentran: Data Source, NGINX y Filebeat.

En la *Figura 7. Componentes SIEM Mozdef* se encuentran los componentes básicos necesarios y los cuales por sus siglas comúnmente se encuentra nombrado como ELK correspondiente a Elastic Search, Logstash y Kibana, a continuación, se describe la funcionalidad que agrega cada componente dentro del SIEM:

12.4.1.1 ElasticSearch. Es un motor de búsqueda distribuido full-text el cual permite realizar búsquedas basadas en niveles de porcentaje y objetos o archivos con contenido de texto, este contenido es estructurado en documentos JSON (*JavaScript Object Notation*) que es un formato de intercambio de datos utilizados por diferentes lenguajes de programación para intercambio de flujos de la información el cual puede ser consultado bajo HTTP (*RESTFull*) es decir mediante la utilización de operaciones como POST, GET, PUT y DELETE.

12.4.1.2 Data Source. Corresponde a las Fuentes de logs otorgadas por los activos de Información. Esta fuente de datos puede presentarse en formato Syslog, Archivos de texto generados por las aplicaciones, redis que son estructuras de datos tipo diccionarios (clave/valor).

12.4.1.3 Logstash. Motor que recopila los datos de diferentes fuentes en tiempo real y los normaliza en el destino de elección. El evento puede ser enriquecido y/o transformado, mediante filtros plugins de entrada y salida.

Logstash está compuesto por Entradas, Filtros y Salidas:

- Entradas: Syslog, *files*, redis, *lumberjack o logstash forwarding.*
- Filtros: procesamiento intermedio con condiciones para realizar una acción en un evento.
  grok: (analiza y estructura texto arbitrario, más de 120 patrones incluidos).
  mutate: (cambia, elimina, modifica campos en los eventos).
  drop: (bloquea eventos completamente por ejemplo eventos *debug).*
  clone: (toma una copia de un evento posiblemente agregando o eliminando campos).
  geoip: (agrega información de ubicación geográfica o direcciones ip).
- *Salidas elasticsearch*: (envía eventos o datos a *elasticsearch*) guarda datos eficientemente.
  files: guarda eventos en un archivo de disco.
  graphite: envía datos a gráficos y almacena métricas.
  statsd: envía eventos a servicio statsd busca contadores y tiempos bajo UDP.

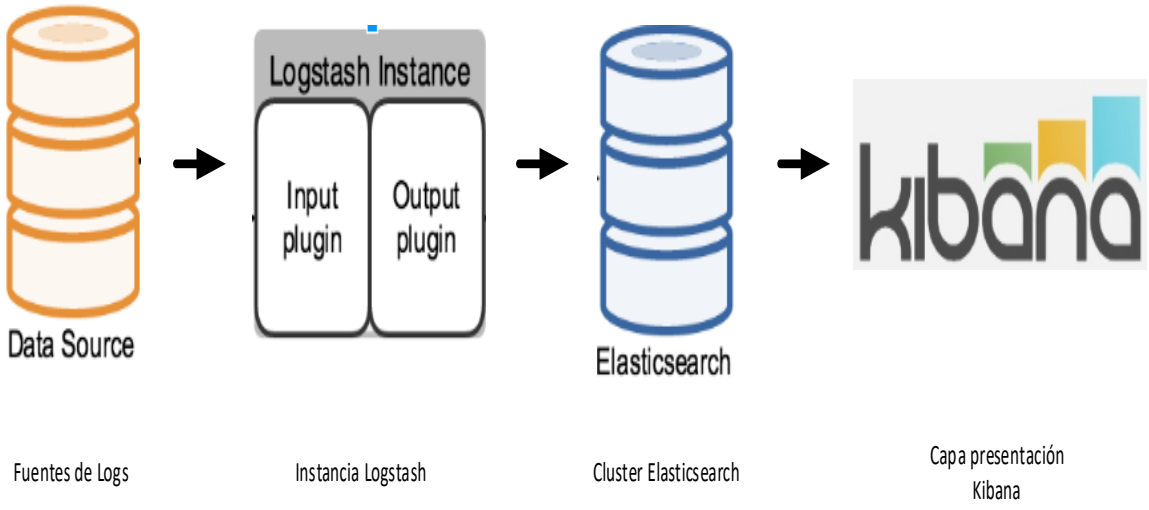
Logstash utiliza codificadores que permiten visualizar o presentar la información en modo consola o debug utilizando lenguajes de intercambio de datos tales como:

Json: decodifica o codifica en formato *json.*
multiline: eventos de texto en múltiples líneas de texto.

12.4.1.4 Kibana. Es una plataforma de visualización de información flexible que permite crear gráficos estadísticos de grandes volúmenes de datos, corresponde a la interface que visualiza el cliente final que recopila la información procesada por *elasticsearch.*

Existen (3) tres arquitecturas de implementación de estos componentes:

Figura 8. Arquitectura Implementación 1

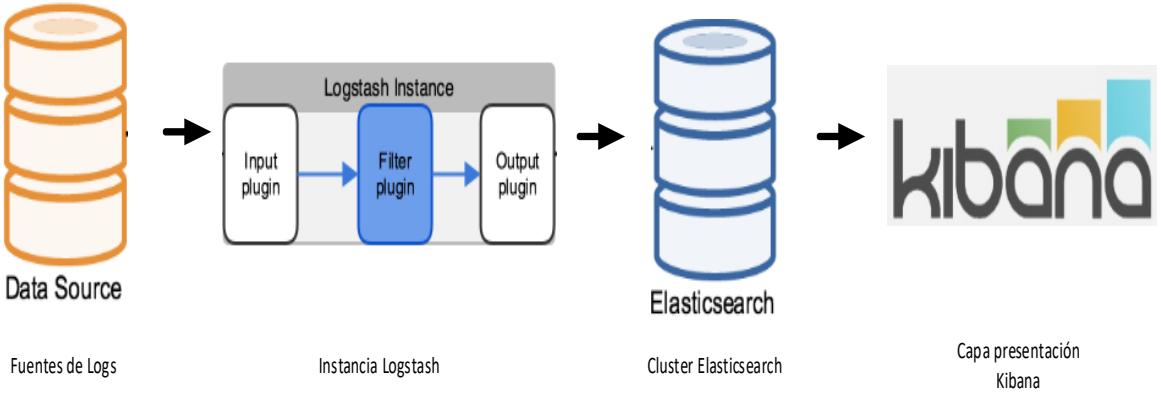


Fuente: www.elasticsearch.com.

La Arquitectura Implementación *1* corresponde a la arquitectura más simple y consiste en un origen de datos (ya sea un servicio, aplicación) que envía los registros directamente a la instancia *Logstash*, esta contiene una entrada y una salida de los registros que son tratados mediante *plugins* (aplicaciones que agregan funcionalidades a otras) para ser normalizados de acuerdo a la aplicación (figura 8).

Cuando los registros ya son normalizados, se envían a *Elasticsearch* el cual cumple con la función de indexar para ejercer búsquedas eficientes. Finalmente, *Kibana* toma la información ya indexada para generar reportes visuales a los administradores.

Figura 9. Arquitectura Implementación 2



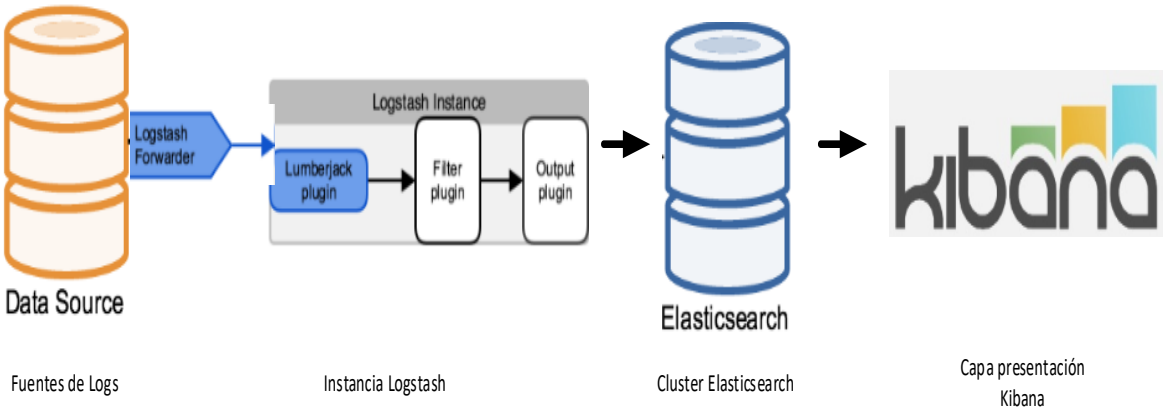
Fuente: www.elasticsearch.com

La arquitectura implementación 2 consiste en un origen de datos (ya sea un servicio, aplicación) que envía los registros directamente a la instancia *Logstash*, esta contiene una entrada, un filtro y una salida de los registros que son tratados mediante *plugins* (aplicaciones que agregan funcionalidades a otras) para ser normalizados de acuerdo a la aplicación (figura 9).

Para este caso el filtro realiza modificaciones o alteraciones sobre los registros mediante el procesamiento de condiciones para depurar la salida.

Cuando los registros ya son normalizados y filtrados, se envían a *Elasticsearch* el cual cumple con la función de indexar para ejercer búsquedas eficientes. Finalmente, *Kibana* toma la información ya indexada para generar reportes visuales a los administradores.

Figura 10. Arquitectura Implementación 3



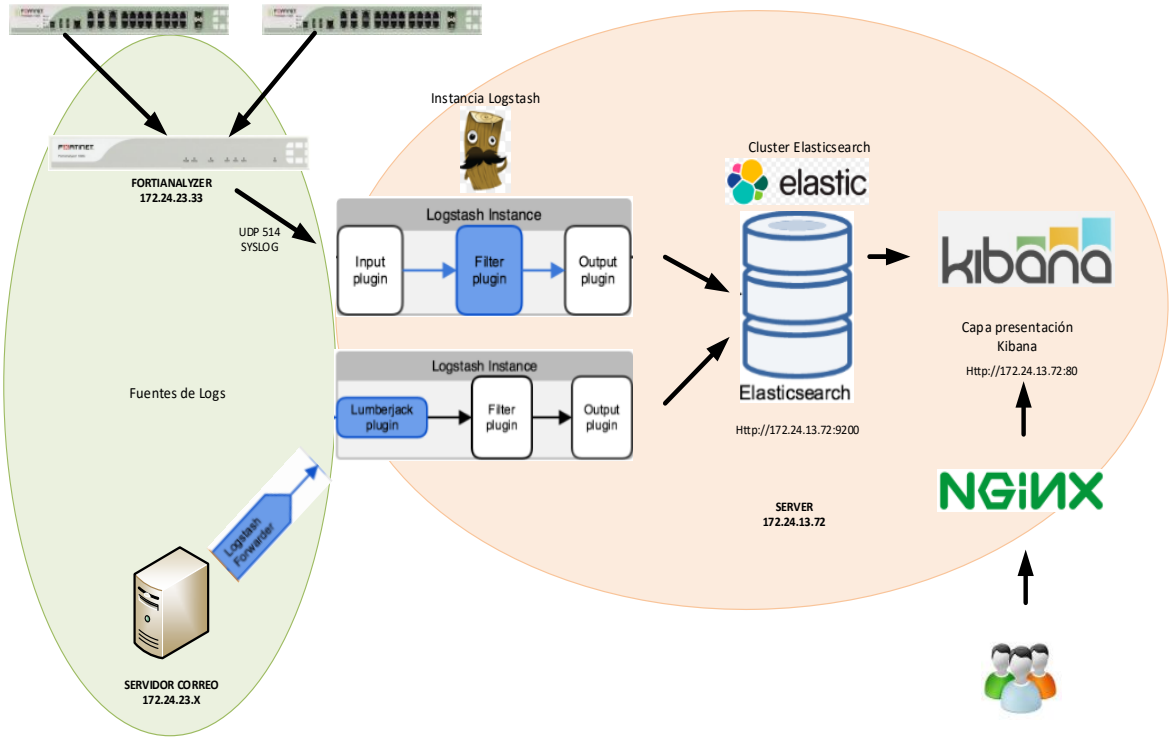
Fuente: www.elasticsearch.com

La Arquitectura Implementación 3 es un origen de datos (ya sea un servicio, aplicación) el cual corre un servicio activo denominado *Logstash Forwarder* donde el registro se procesa directamente desde el origen (requerido regularmente cuando la carga del registro es bastante grande y necesita comprimir esta información), luego es recibida por el *plugin Lumberjack* el cual descomprime y continua su funcionamiento normal enviándolo hacia el filtro y una salida de los registros que son tratados mediante *plugins* (aplicaciones que agregan funcionalidades a otras) para ser normalizados de acuerdo a la aplicación (figura 10).

Para este caso el filtro realiza modificaciones o alteraciones sobre los registros mediante el procesamiento de condiciones para depurar la salida. Cuando los registros ya son normalizados y filtrados, se envían a *Elasticsearch* el cual cumple con la función de indexar para ejercer búsquedas eficientes. Finalmente, *Kibana* toma la información ya indexada para generar reportes visuales a los administradores.

Basados en lo anterior y la necesidad del cliente, para el presente proyecto se estableció una Arquitectura híbrida compuesta por lumberjack y logstash con la utilización de filtros.

Figura 11. Arquitectura implementada en la Armada



Fuente: Los autores, 2016.

La Arquitectura implementada en la Armada, se desarrolló el diagrama de Infraestructura con los componentes necesarios para el funcionamiento del SIEM y los dispositivos o servicios integrados inicialmente de acuerdo al alcance del proyecto (figura 11*)*, dentro de los componentes se encuentran:

Firewall*: d*ispositivo de seguridad perimetral que analiza el tráfico entrante y saliente utilizado para bloquear accesos no autorizados a la infraestructura de la Armada, estos sistemas se encuentran en alta disponibilidad protegiendo la zona DMZ donde se encuentran servidores publicados o expuestos a Internet así mismo protege otra zona definida para la Granja de Servidores internos la cual también se encuentra protegida por estos dispositivos (figura 12).

Figura 12. Firewall

Fuente: www.fortinet.com.

Analyzer: este dispositivo envía paquetes al servidor mediante la utilización de protocolos estándar como Syslog compuesto por una prioridad, cabecera y payload definidos en la RFC 5424, esta una de las principales fuentes de origen de información o *Data Source* utilizados por el SIEM.

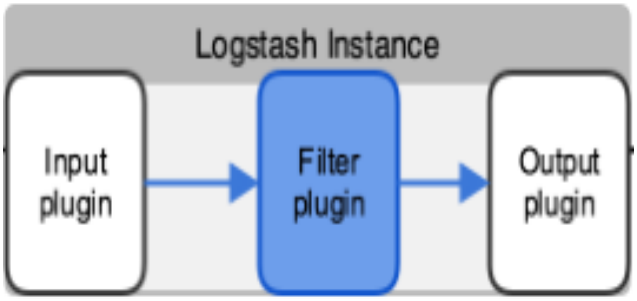
Figura 13. Analyzer

Fuente: www.fortinet.com.

*Analyzer c*orresponde a un dispositivo o *Appliance* que tiene la función de centralizar los logs de los dispositivos firewall, Firewall de aplicaciones, equipo de denegación de servicio y páginas WEB (figura 13).

Instancia *Logstash:* Se visualizan los módulos que hacen parte del componente de *Logstash*, este se encarga de recopilar los datos en tiempo real del *Analizer* y los servidores integrados con el SIEM (figura 14).

Figura 14. Instancia Logstash



Fuente: www.elasticsearch.com

La información es recibida desde el Analyzer (*figura 13. Analyzer)* Mediante el *plugin* de entrada, este plugin es configurado con parámetros de formato tipo *syslog* en el puerto personalizado para este servicio (UDP 1514) y el plugin de salida se encarga de entregar esta información normalizada al siguiente componente que es Elasticsearch.

Elasticsearch: Componente encargado de la indexación del contenido es *Elasticsearch* (figura 15).

Figura 15. Elasticsearch

Fuente: www.elasticsearch.com.

Elasticsearch es un motor que realiza la búsqueda de eventos recibidos por *Logstash.* Los eventos son estructurados y pueden ser visualizados en formato de intercambio de datos JSON a través del servicio publicado en el puerto 9200.

Kibana: el Componente de Kibana (figura 16). *Kibana* se encarga de interpretar los datos recibidos por *Elasticsearch* para presentar los gráficos estadísticos de forma visual mediante *Dashboards* personalizables.

Figura 16. Kibana

Fuente: www.elasticsearch.com.

Kibana permite a través de su interfaz la utilización de filtros que realizan búsquedas y correlaciona los eventos de cada objeto o elemento de la infraestructura de la Armada, estos eventos son previamente indexados por *Elasticsearch.*

***Nginx**: e*ste componente permite realizar la autenticación de los usuarios de la Armada con permisos para realizar la consulta de la información a través de *Kibana*. Básicamente es un Servidor Proxy instalado con la finalidad de proporcionar seguridad para consultar los servicios HTTP publicados en el servidor (figura 17).

Figura 17. Nginx

Fuente: www.nginx.org.

Consulta de usuarios registrados: Finalmente, en el diagrama se representan los usuarios permitidos o autorizados para consultar la aplicación a través de *Kibana* (figura 18).

Figura 18. Usuario

Fuente: www.microsoft.com

12.5 IMPLEMENTACIÓN

De acuerdo a la documentación de los fabricantes del producto y las necesidades de la Armada se realiza la fase de implementación, donde se define inicialmente el modo de instalación para lo cual existen 3 tipos *Cloud, Hybrid o Self Hosted*.

Para lo anterior se debe tener en cuenta que los equipos que se integran al SIEM se encuentran ubicados localmente en el *datacenter* de la Armada, por seguridad

no se encuentran compartiendo la Infraestructura en la nube o utilizan *clouds* públicas para este tipo de servicios.
Así mismo el fabricante del producto SIEM recomienda que el servidor se encuentre dentro de la misma zona o ubicación, con la menor latencia posible que no supere en lo posible 250 ms con el fin de garantizar la entrega de los paquetes y tiempos de procesamiento de la información.

Basados en los anteriores conceptos y requerimientos se define que la plataforma se instalará en modo *Self Hosted*, en un servidor físico en el interior del d*atacenter* de la Armada.

12.5.1 Definición de recursos. Se estableció una primera reunión con la Armada con el fin de presentar la solución y de acuerdo al alcance identificar los recursos necesarios para empezar con la implementación. Dentro de los recursos identificados se encuentran:

- Un servidor con las características necesarias para la implementación.
- Un acceso VPN para realizar conexión segura y configuraciones.
- Alcanzabilidad de red desde el servidor hacia los elementos que se integrarán a la solución SIEM o acceso a orígenes de datos.
- Direccionamiento de red, Nombre de Host y otros parámetros que designe la armada para integrar el servidor en la red.

12.5.1.1 Características del servidor. Para desplegar *Elasticsearch* en un ambiente de producción, el fabricante de las principales herramientas sugiere una serie de recursos, sin ser un obligatorio cumplimiento puesto que depende de la cantidad de equipos de recolección, tareas y servicios implementados, sin embargo, es un buen punto de partida atender las siguientes recomendaciones:

Memoria: se recomienda no utilizar una memoria inferior a 8GB y no mayor a 64 GB, es posible utilizar memoria adicional utilizando caché en el Disco duro o sistema de archivos.

Disco Duro: Es importante para los procesos de indexación que requieren lectura, por lo cual se recomienda la utilización de discos SSD o discos duros de 15k RPM, evitar igualmente almacenamiento conectado a red como NAS.

Red: Se recomienda una red de baja latencia para aseguramiento de comunicación entre los nodos, considerar conexiones de 1GB mínimo.

CPUs: En *clusters* comunes se utilizan máquinas con dos hasta ocho núcleos.

Inicialmente para el proyecto se dispuso de una Máquina Virtual, la cual no contaba con los recursos necesarios de espacio en disco duro, por lo cual la Armada dispuso de una Máquina Física con las siguientes características:

Memoria RAM: 4000 Mb.
Memoria virtual: 4000 Mb.
Disco Duro: 1,7 TB.
Procesador: Intel X86_64 2.1 GHz, dos núcleos.
Network: 1 GbE.

El sistema operativo para el *host* físico se configuró teniendo en cuenta la matriz de compatibilidad (figura 19). La cual el fabricante determina con el fin de garantizar el correcto funcionamiento de las herramientas y el soporte brindado:

Figura 19. Matriz de compatibilidad Sistemas Operativos

Product and Operating System

	CentOS/RHEL 6.x/7.x	Oracle Enterprise Linux 6/7 with RHEL Kernel only	Ubuntu 12.04/14.04	SLES 11 SP4**/12	OpenSuSE 13.2	Windows Server 2012/R2	Windows Server 2008	Debian 7	Solaris/SmartOS	Amazon Linux*
Elasticsearch 1.5.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖
Elasticsearch 1.6.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖
Elasticsearch 1.7.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖
Elasticsearch 2.0.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✔
Elasticsearch 2.1.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✔
Elasticsearch 2.2.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✔
Elasticsearch 2.3.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✔
Elasticsearch 2.4.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✔
Logstash 1.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖
Logstash 2.0.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖
Logstash 2.1.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖
Logstash 2.2.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖
Logstash 2.3.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖
Logstash 2.4.x	✔	✔	✔	✔	✔	✔	✖	✔	✖	✖

Fuente: https://www.elastic.co/support/matrix.

El sistema operativo instalado se encuentra inmerso dentro de la matriz de compatibilidad el cual se configuró con los siguientes parámetros:

Sistema operativo: Ubuntu server 14.04 TLS.
Dirección IP: 172.24.XX.XX.
Hostname: kraken.

12.5.2 Instalación y configuración. Teniendo los recursos se realiza el proceso de Instalación, a continuación, se describen las versiones de los paquetes y productos instalados, listado de servicios que deben estar en ejecución, permisos configurados en el cortafuegos, instalación de paquetes y configuración de los mismos, rutas de archivos de configuración y pruebas de los servicios. Para el siguiente proyecto se utilizaron las siguientes versiones de paquetes instalados:

12.5.2.1 Versiones de los paquetes y productos instalados. Para el siguiente proyecto se utilizaron las siguientes versiones de paquetes instalados:

Linux Ubuntu Server 14.04.
Elasticsearch 2.0.0-1.
Logstash.noarch 2.0.0-1.
httpd apache 2.4.6.
kibana.x86_64 4.3.0.
nginx 2.0.0.
Java 8.

12.5.2.2 Listado de servicios. Es necesario que los siguientes servicios se mantengan en ejecución en el servidor y permitir que la herramienta permanezca disponible para su consulta:

Httpd: se encarga de coordinar los procesos del servidor Apache HTTP.

Elasticserch: se encarga de los procesos de indexación y motores de búsqueda.

***Logstash*:** se encarga de los procesos de recopilación de datos y normalización.

Kibana: se encarga de mantener la plataforma de visualización.

12.5.2.3 Permisos en cortafuegos. UFW es una herramienta del sistema operativo Linux Ubuntu para configurar reglas fácilmente en los *iptables firewall*, por defecto se encuentra deshabilitado sin embargo es posible su activación mediante el comando *sudo ufw enable.* Para permitir el acceso a los puertos requeridos por las herramientas que componen el SIEM se ejecutaron los siguientes comandos:

sudo ufw allow http: Permite ofrecer permisos para consultar el puerto 80 necesario para publicar el servicio de kibana.

sudo ufw allow https: Permite ofrecer permisos para consultar el Puerto 443 necesario para publicar el servicio de kibana con protocolo seguro.

sudo ufw allow 514/tcp: Puerto utilizado por *Logstash* y utilizado por syslog con el fin de recibir mensajes de registro.

sudo ufw allow 514/udp: Puerto utilizado por *Logstash* y utilizado por syslog con el fin de recibir mensajes de registro.

sudo ufw allow 3514/tcp: Puerto utilizado por *Logstash* definido para recibir mensajes tipo syslog desde el equipo *Fortigate*.

sudo ufw allow 9200/tcp: Puerto utilizado por *Elasticsearch* para realizar la consulta del estado de los índices a través de Restful permitiendo operaciones como *GET, POST, PUT, DELETE*.

sudo ufw allow OpenSSH: Permite acceder al servidor vía SSH a través del puerto 2222.

12.5.2.4 Instalación de paquetes y configuración.

sudo apt-get update: Este comando permite realizar la actualización de repositorios o la lista de paquetes disponibles y sus correspondientes versiones definidos en el *source.list* (necesario cada vez que se actualiza un repositorio).

sudo add-apt-repository -y ppa:webupd8team/java: Este comando agrega en el repositorio los paquetes disponibles para Java versión 8.

sudo apt-get -y install oracle-java8-installer: Este paquete es recomendado por el fabricante para la ejecución de E*lasticsearch*, documentado en su página web: https://www.elastic.co/guide/en/elasticsearch/reference/2.3/_installation.html

wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -: Permite la creación de claves simétricas para el cifrado de mensajes en donde se requiere la utilización de nodos *Elasticsearch* que conforman un cluster.

echo "deb http://packages.elastic.co/elasticsearch/2.x/debian stable main" | sudo tee -a /etc/apt/sources.list.d/elasticsearch-2.x.list: Permite agregar dentro del archivo *source.list* el repositorio necesario para la descarga e instalación de paquetes de *Elasticsearch*.

sudo apt-get update: Este comando permite realizar la actualización de repositorios o la lista de paquetes disponibles y sus correspondientes versiones definidos en el *source.list* (necesario cada vez que se actualiza un repositorio).

sudo apt-get -y install elasticsearch: Realiza la instalación de los paquetes necesarios del componente de *Elasticsearch*.

sudo vi /etc/elasticsearch/elasticsearch.yml: Edita el archivo de configuración de *Elasticsearch* en donde se configura el siguiente parámetro: network.host: *localhost*

sudo service elasticsearch restart: reinicia el servicio de *Elasticsearch* es necesario cuando se edita algún parámetro del archivo de configuración *elasticsearch.yml*

sudo update-rc.d elasticsearch defaults 95 10: asegura que el servicio *Elasticsearch* se inicie cuando el sistema operativo se encuentre en el proceso de arranque.

sudo groupadd -g 999 kibana: agrega el grupo de usuarios Kibana en el sistema operativo.

sudo useradd –u 999 –g 999 kibana: agrega el usuario Kibana dentro del grupo denominado también Kibana utilizado para la ejecución del servicio.

cd ~; wget https://download.elastic.co/kibana/kibana/kibana-4.3.0-linux-x64.tar.gz**:** realiza la descarga del paquete de Kibana desde el sitio oficial del fabricante.

tar xvf kibana-*.tar.gz: permite extraer el paquete anteriormente descargado.

vi ~/kibana-4*/config/kibana.yml: Edita el archivo de configuración de Kibana en donde se configura el siguiente parámetro: *server.host: "localhost"*

sudo mkdir -p /opt/kibana: permite crear un directorio en la ruta /opt/kibana.

sudo cp -R ~/kibana-4*/* /opt/kibana/: Copia todo el contenido de la carpeta actual y lo pega en la carpeta de destino /opt/kibana.

sudo chown -R kibana: /opt/kibana: Permite asegurarse que el propietario de la información contenida en la ruta /opt/kibana es el usuario creado anteriormente “kibana”.

cd /etc/init.d && sudo curl -o kibana https://gist.githubusercontent.com/thisismitch/8b15ac909aed214ad04a/raw/fc5025c3fc499ad8262aff34ba7fde8c87ead7c0/kibana-4.x-init permiten descargar un script inicial de configuración de Kibana.

cd /etc/default && sudo curl -o kibana https://gist.githubusercontent.com/thisismitch/8b15ac909aed214ad04a/raw/fc5025c3fc499ad8262aff34ba7fde8c87ead7c0/kibana-4.x-default permiten descargar un script inicial de configuración por defecto de Kibana.

sudo chmod +x /etc/init.d/kibana: permite generar permisos de ejecución sobre el archivo del servicio.

sudo update-rc.d kibana defaults 96 9: asegura que el servicio Kibana se inicie cuando el sistema operativo se encuentre en el proceso de arranque.

sudo service kibana start: inicia el servicio de elasticsearch es necesario cuando se edita algún parámetro del archivo de configuración kibana.yml ejecutar con el parámetro restart.

sudo apt-get install nginx apache2-utils: Instala un servidor Proxy reverse que sirve para proteger el acceso mediante un usuario y contraseña a los requerimientos HTTP que se realicen contra el host.

sudo htpasswd -c /etc/nginx/htpasswd.users ArmadaMil: permite utilizar htpasswd como los usuarios permitidos para autenticarse a los requerimientos HTTP.

sudo vi /etc/nginx/sites-available/default: Edita el archivo de configuración de Kibana en donde se configuran los siguientes parámetros:

```
server {
    listen 80;
    server_name elksiem;
    auth_basic "Restricted Access";
    auth_basic_user_file /etc/nginx/htpasswd.users;
    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

sudo service nginx restart: reinicia el servicio de *nginx* es necesario cuando se edita algún parámetro del archivo de configuración default.

echo 'deb http://packages.elasticsearch.org/logstash/2.1/debian stable main' | sudo tee /etc/apt/sources.list.d/logstash.list: Permite agregar dentro del archivo *source.list* el repositorio necesario para la descarga e instalación de paquetes de *Logstash*.

sudo apt-get update: Este comando permite realizar la actualización de repositorios o la lista de paquetes disponibles y sus correspondientes versiones definidos en el *source.list* (necesario cada vez que se actualiza un repositorio).

sudo apt-get install logstash: Realiza la instalación de los paquetes necesarios del componente *Logstash*.

sudo mkdir -p /etc/pki/tls/certs: Crea un directorio donde se almacenarán los certificados de seguridad SSL.

sudo mkdir /etc/pki/tls/private: crea un directorio donde se almacenarán las llaves privadas de los certificados.

sudo vi /etc/ssl/openssl.cnf: edita el archivo de configuración utilizado como plantilla para la generación de los certificados, en el cual se agregan los siguientes parámetros, para este caso la dirección IP del servidor:

[v3_ca]
subjectAltName = IP: 172.24.xx.xx

cd /etc/pki/tls
sudo openssl req -config /etc/ssl/openssl.cnf -x509 -days 3650 -batch -nodes -newkey rsa:2048 -keyout private/logstash-forwarder.key -out certs/logstash-forwarder.crt: este comando permite generar los certificados SSL en base a la plantilla de configuración y la llave privada.

sudo vi /etc/logstash/conf.d/02-filebeat-input.conf: edita los archivos de configuración utilizados por *Logstash* mediante los filtros de entrada y salida de eventos.

La siguiente configuración permite la utilización del puerto 5044 para obtener los eventos del recolector *Forti Analyzer*, utilizando el certificado de seguridad generado anteriormente.

```
Input {
 beats {
    port => 5044
    type => “logs”
    ssl => true
    ssl_certificate => “/etc/pki/tls/certs/logstash-forwarder.crt”
    ssl_key => “/etc/pki/tls/private/logstash-forwarder.key”
  }

}
```

sudo vi /etc/logstash/conf.d/10-syslog.conf: edita el archivo de configuración de Logstash que permite realizar un filtro para reconocer el origen del evento, fecha y hora específica en un formato determinado.

```
filter {
  if [type] == "syslog" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp}
%{SYSLOGHOST:syslog_hostname}
%{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?:
%{GREEDYDATA:syslog_message}" }
      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
    }
    syslog_pri { }
    date {
      match => [ "syslog_timestamp", "MMM  d HH:mm:ss", "MMM dd HH:mm:ss" ]
    }

  }
}
```

sudo vi /etc/logstash/conf.d/30-elasticsearch-output.conf: edita el archivo de configuración de *logstash* que permite que se genere la salida de eventos en el servicio de *elasticsearch* para posteriormente realizar procesos de indexación de la información. El cual contiene la siguiente configuración:

```
output {
  elasticsearch { hosts => ["localhost:9200"] }
  stdout { codec => rubydebug }
}
```

sudo service logstash restart: reinicia el servicio de Logstash es necesario cuando se edita algún parámetro del archivo de configuración ubicados en la ruta /etc/logstash/conf.d/.

sudo update-rc.d logstash defaults 96 9: asegura que el servicio Logstash se inicie cuando el sistema operativo se encuentre en el proceso de arranque.

scp /etc/pki/tls/certs/logstash-forwarder.crt mozdef@172.24.x.x: /tmp:
Realiza un acopio o respaldo de los certificados de seguridad.

echo "deb https://packages.elastic.co/beats/apt stable main" | sudo tee -a /etc/apt/sources.list.d/beats.list: permite agregar dentro del archivo source.list el

repositorio necesario para la descarga e instalación de paquetes del componente Filebeat.

wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –: instala conjunto de llaves GPG-KEY para el intercambio seguro de entre el servidor de descarga y el *host* donde se instala la aplicación.

sudo apt-get update: este comando permite realizar la actualización de repositorios o la lista de paquetes disponibles y sus correspondientes versiones definidos en el *source.list* (necesario cada vez que se actualiza un repositorio).

sudo apt-get install filebeat: instala los paquetes necesarios para la instalación de filebeat el cual permite administrar y procesar las colas para envío a Logstash.

sudo mkdir -p /etc/pki/tls/certs
sudo cp /tmp/logstash-forwarder.crt /etc/pki/tls/certs/. Crea carpeta donde se almacenan los certificados para logstash.

sudo vi /etc/filebeat/filebeat.yml: edita el archivo de configuración de Filebeat en el cual se agrega el parámetro de configuración de Host.

sudo service filebeat restart: reinicia el servicio de Filebeat es necesario cuando se edita algún parámetro del archivo de configuración ubicados en la ruta /etc/filebeat/filebeat.yml.

sudo update-rc.d filebeat defaults 95 10: asegura que el servicio Logstash se inicie cuando el sistema operativo se encuentre en el proceso de arranque.

12.5.2.5 Rutas de archivos de configuración. A continuación, se consolidan las rutas de acceso a los archivos de configuración de cada uno de los componentes:

Servidor Apache: httpd.conf.
Elasticssearch: /etc/elasticsearch/elasticsearch.yml.
Nginx: /etc-nginx/sites-available/default.
Kibana: /opt/kibana/config/kibana.yml.
Logstash: /etc/logstsh/conf.d/10-syslog.conf.
Logstash-Filebeat: /etc/logstsh/conf.d/02-filebit-input.conf.
Logstash-Elasticsearch: /etc/logstsh/conf.d/30-elasticsearch-output.conf.
Collectd: /etc/collectd/collect.conf.
Filebeat: /etc/filebeat/filebeat.yml.
Indices Elasticsearch: /var/lib/elasticsearch/elasticsearch/nodes/0/índices.

12.5.2.6 Pruebas de funcionamiento de los servicios. Las siguientes instrucciones o comandos permiten ejecutar pruebas sobre los servicios instalados:

http://localhost:9200/_cat/indices?v: Con el fin de verificar el funcionamiento de Elasticsearch es posible visualizar el listado de índices a través de esta URL.
du -hlsc /var/log/elasticsearch: Permite identificar el tamaño de las carpetas de elasticsearch.

sudo service logstash configtest: Permite ejecutar *logstash* en modo *debug* para visualizar los mensajes recibidos.

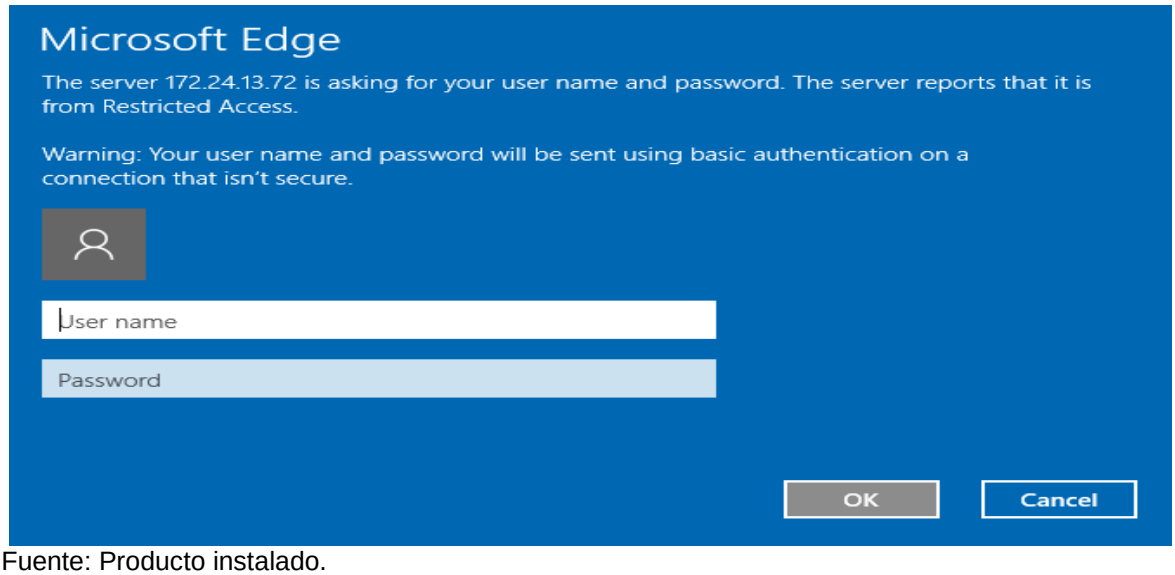
12.5.2.7 Documentación. Para el presente proyecto se elaboró un manual de usuario el cual fué entregado al personal responsable de operar la herramienta, dicho manual está orientado específicamente al SIEM instalado en la Armada.

12.6 RESULTADOS

Posteriormente a las fases de Diseño, implementación y pruebas, se presenta una fase de resultados donde se evidencia la operación del SIEM.

La Autenticación *SIEM*. Se visualiza que el servidor Proxy se encarga de realizar el proceso de autenticación utilizando un usuario y contraseña definidos previamente con el fin de acceder al componente kibana que presenta la información recolectada (figura 20):

Figura 20. Autenticación SIEM

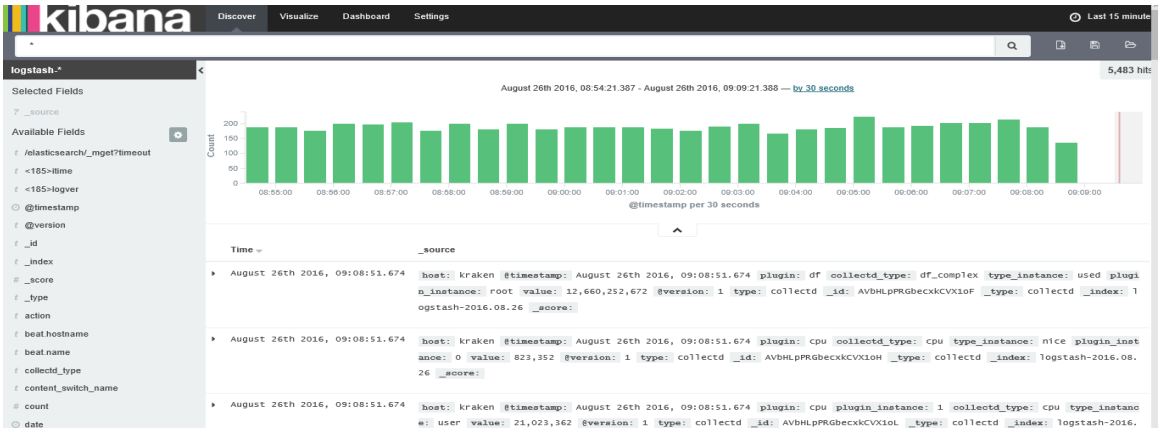


Fuente: Producto instalado.

En la figura 21, se identifica la primera pestaña del sistema la cual permite visualizar la recolección de eventos capturados en línea de tiempo.

En la parte inferior se encuentra la descripción de cada registro o log que se está almacenando en tiempo real y sobre el borde izquierdo cada uno de los campos que están disponibles previamente indexados y normalizados por los servicios de *Logstash y Elasticsearch*.

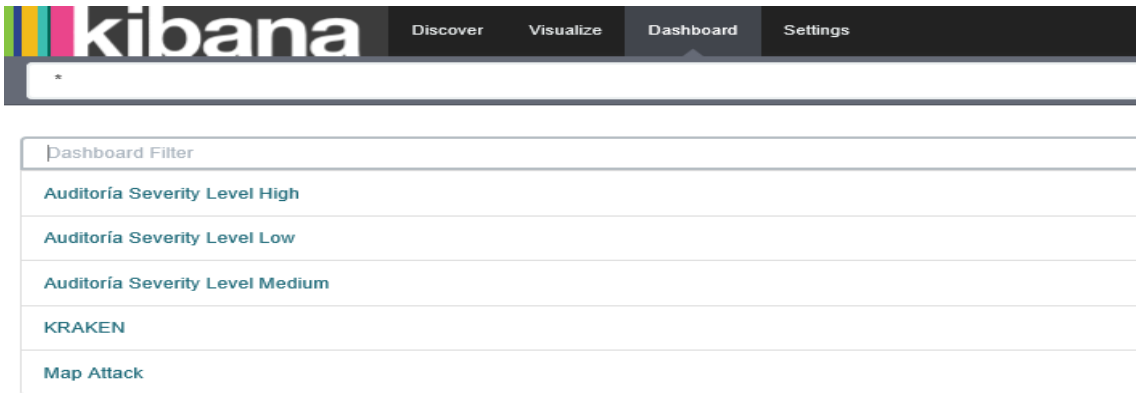
Figura 21. Recolección de eventos



Fuente: Producto instalado.

En la pestaña denominada *Dashboard* en la figura 22, es posible crear vistas que permiten crear Paneles de visualización personalizados. En el caso de la Armada se crearon *Dashboards* a la medida que permiten visualizar los riesgos potenciales, categorizados por Niveles Bajo, Medio y Alto, así mismo un panel que permite visualizar el estado de los recursos de los servidores agregados y el mapa con la geolocalización de los ataques.

Figura 22. Niveles de riesgo



Fuente: Producto instalado.

Al abrir el *Dashboard* crítico, le permite a la Armada contar con un panorama visible, obteniendo información de los recursos frente a un eventual ataque informático. En la figura 23, es posible identificar:

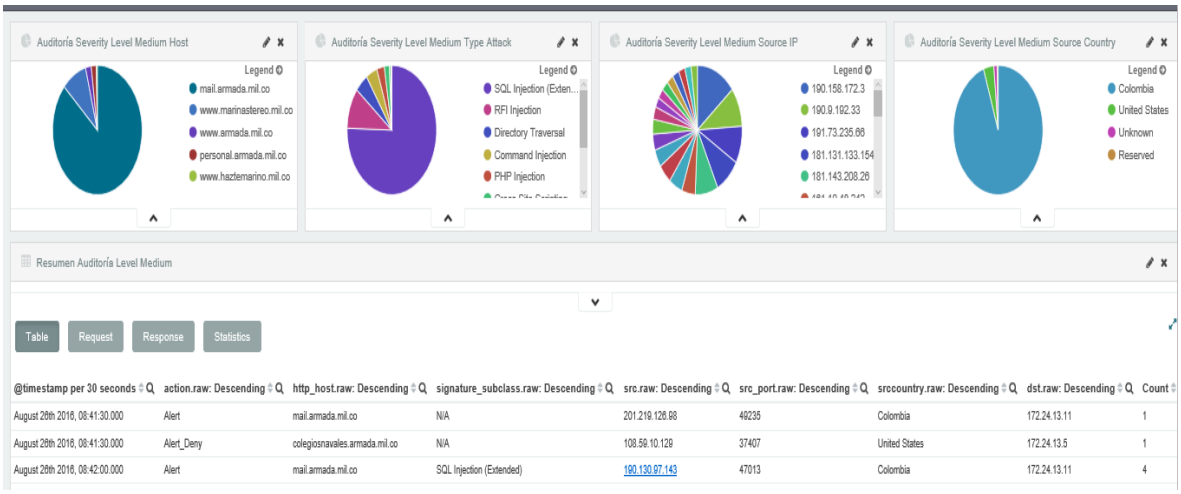
- Top 10 del tipo de ataques.
- Top 10 de direcciones IP fuente de donde se originó el ataque, con el fin de contribuir a los análisis forenses de la Armada.
- Top 10 de los países de donde se originan los ataques.
- Top 10 de los recursos atacados.

Figura 23. Top 10

Fuente: Producto instalado.

En el *dashboard* también se puede identificar la tabla de donde se obtienen los datos para generar el gráfico de forma más detallada. En las columnas se encuentran los campos de fecha y hora, host, tipo de ataque, dirección IP fuente, puerto, Ciudad, dirección IP destino (figura 24).

Figura 24. Datos gráficos



Fuente: Producto instalado

Es posible identificar un dashboard configurado para identificar geográficamente los puntos origen desde donde se produce el ataque (figura 25) y con una coloración que se va haciendo intensa al tener un mayor número de eventos, conforme se visualiza en la siguiente imagen:

Figura 25. Geolocalización

Fuente: Producto instalado.

En el sistema también se puede monitorear el estado de los recursos de los servidores (figura 26) que se deben agregar, esto con el fin de evidenciar si se presenta agotamiento de los mismos. En el panel se puede identificar:

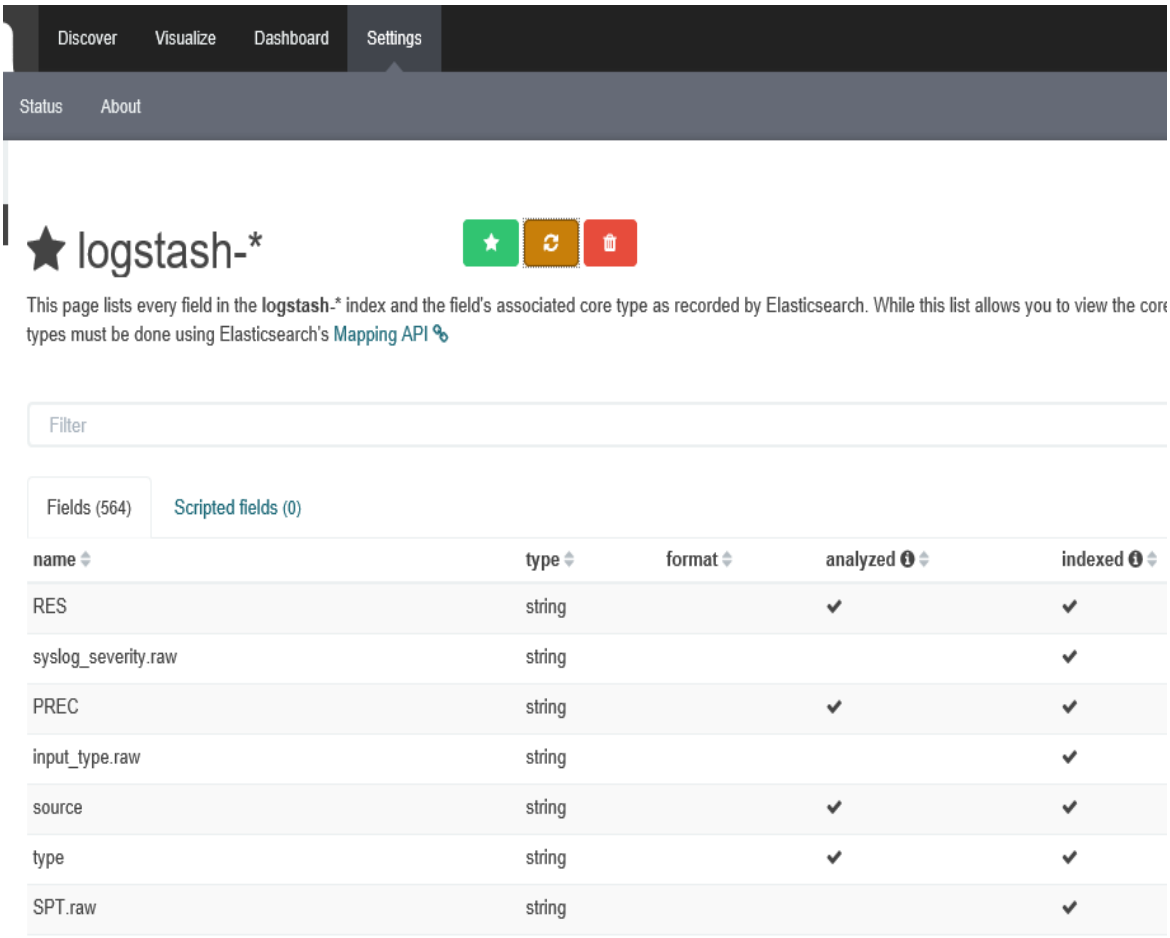
- Estado de CPU.
- Memoria.
- Disco Duro.

Figura 26. Monitoreo estado de recursos

Fuente: Producto instalado.

Mediante la recaudación histórica de eventos el sistema permite aprender nuevos índices que mejoran las búsquedas y filtros de información. En la pestaña *Settings* se actualizan los campos disponibles de cada recurso monitoreado (figura 27).

Figura 27. Índices



Fuente: Producto instalado.

En la figura 28, se visualizan los periodos en los que el administrador tiene la posibilidad de presentar las estadísticas o información recolectada de los *dashboards* configurados.

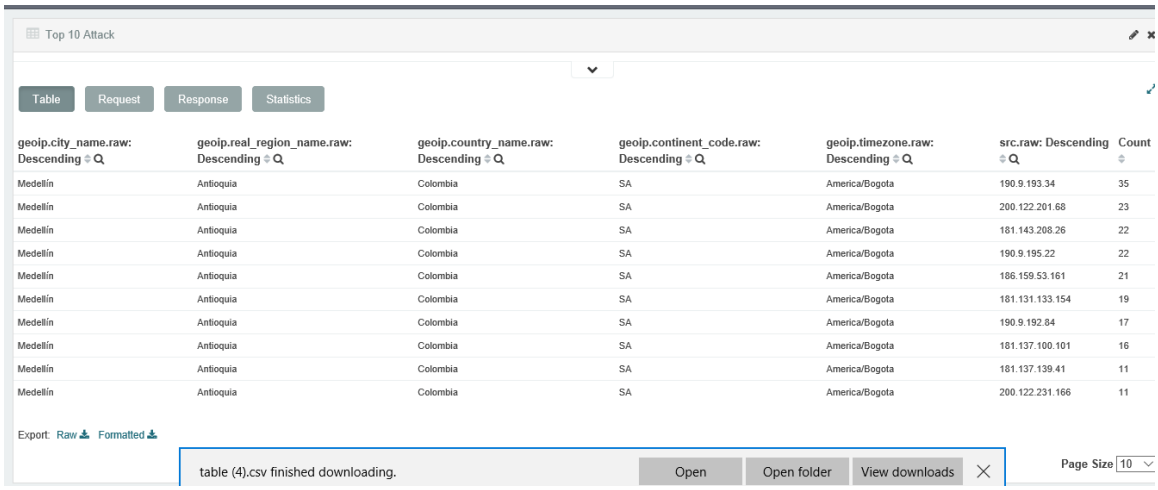
Así mismo en la parte inferior le permite obtener mediante un gráfico de barras la cantidad de eventos presentados en tiempo real del sistema que se está monitoreando, con lo cual puede identificar fácilmente si existe una caída de registro de eventos o algún tipo de sobre taza con respecto a la cantidad de eventos que se generan regularmente.

Figura 28. Estadísticas periodos de tiempo.

Fuente: Producto instalado.

La información es posible presentarla tabulada, con la posibilidad de organizarla por el nombre de columna tal como se enseña en la figura 29, permite personalizar la cantidad de resultados por página; en su parte inferior se presenta un link que permite descargarla o exportarla.

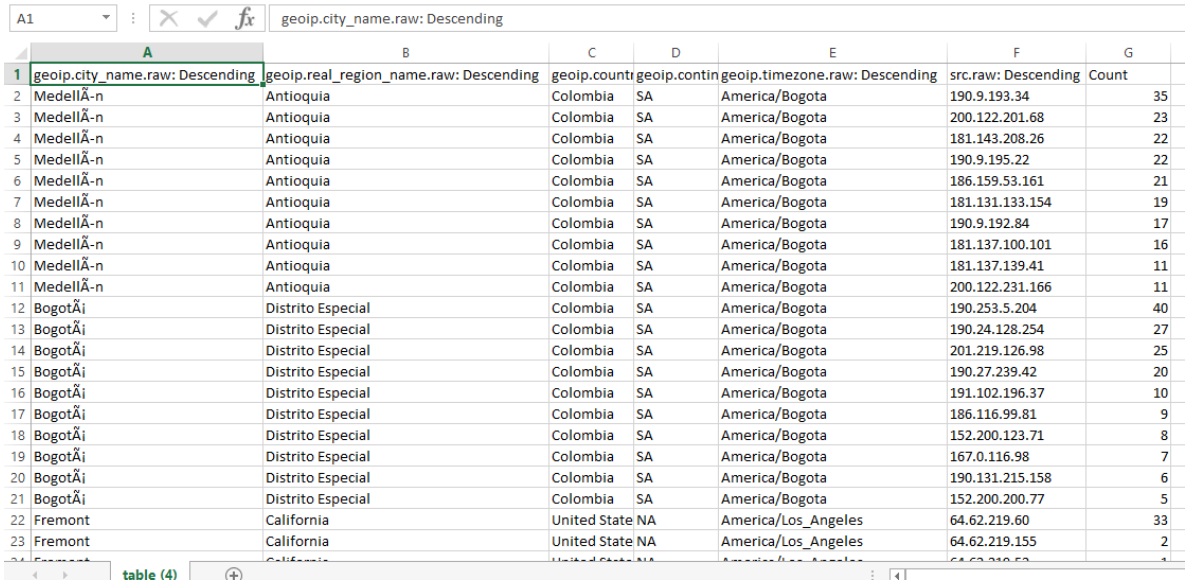
Figura 29. Exportación de información



Fuente: Producto instalado.

La información es posible exportarla en formato CSV (valores separados por comas) para su posterior análisis y la cual se puede llevar a un libro de Excel como se indica en la figura 30.

Figura 30. Exportación CSV



	A	B	C	D	E	F	G
1	geoip.city_name.raw: Descending	geoip.real_region_name.raw: Descending	geoip.countr	geoip.contin	geoip.timezone.raw: Descending	src.raw: Descending	Count
2	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	190.9.193.34	35
3	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	200.122.201.68	23
4	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	181.143.208.26	22
5	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	190.9.195.22	22
6	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	186.159.53.161	21
7	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	181.131.133.154	19
8	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	190.9.192.84	17
9	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	181.137.100.101	16
10	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	181.137.139.41	11
11	MedellÃ-n	Antioquia	Colombia	SA	America/Bogota	200.122.231.166	11
12	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	190.253.5.204	40
13	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	190.24.128.254	27
14	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	201.219.126.98	25
15	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	190.27.239.42	20
16	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	191.102.196.37	10
17	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	186.116.99.81	9
18	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	152.200.123.71	8
19	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	167.0.116.98	7
20	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	190.131.215.158	6
21	BogotÃ¡	Distrito Especial	Colombia	SA	America/Bogota	152.200.200.77	5
22	Fremont	California	United State	NA	America/Los_Angeles	64.62.219.60	33
23	Fremont	California	United State	NA	America/Los_Angeles	64.62.219.155	2

Fuente: Producto instalado.

Igualmente es posible identificar el nivel de carga del servidor, esto con el fin de ir realizando una auditoria del mismo servidor. En la figura 31*,* en la parte superior se presenta el estado, en donde:

Green: indica que el servidor se encuentra operativo y con los recursos estables.

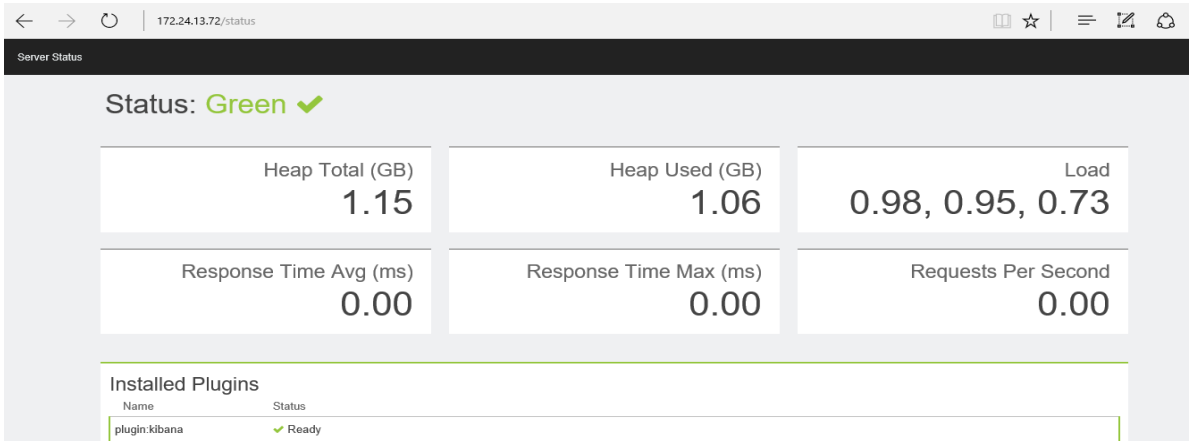
Yellow: indica una advertencia a la cual el administrador debe intervenir y tomar alguna acción.

Red: indica que algún servicio se detuvo, los tiempos de respuesta se encuentran muy altos o los recursos del servidor no responden.

Para lo anterior el sistema se basa en datos obtenidos con respecto a los promedios de tiempo de respuesta de indexación, respuestas por segundo, estado de la memoria y el procesamiento.

Dichos valores se presentarán en color rojo también, en caso que genere una advertencia o caída identificando con certeza la causa.

Figura 31. Carga del servidor



Fuente: Producto instalado.

12.7 ANÁLISIS DE RESULTADOS

En la tabla 2, es posible identificar claramente que los tipos de ataques con mayor cantidad de registros evidenciados en la Armada corresponden a los siguientes en orden de mayor a menor:

Tabla 2. Top 10 Ataques

Top/posición	Tipos de ataque
1	Cross site scripting
2	Command injection
3	Directory trasversal
4	PHP Injection
5	N/A
6	SQL Injection
7	Bad Robot
8	HTTP Response Spliting
9	OS Command Injection
10	Credit card Detection

Fuente: Producto SIEM implementado.

La Armada también cuenta con la posibilidad de identificar las direcciones IP fuentes que más han generado ataques y de esta forma generar mecanismos preventivos que les permita ejecutar acciones proactivas frente ellos:

Tabla 3. Top 10 Direcciones IP atacantes

Top/Posición	Direcciones Fuente
1	190.158.172.3
2	181.148.175.88
3	161.18.44.216
4	190.9.192.33
5	190.130.97.143
6	190.242.73.222
7	181.143.208.26
8	191.155.184.79
9	191.73.235.66
10	190.130.103.87

Fuente: Producto SIEM implementado.

En la tabla 3, se identifica que la mayoría de las direcciones IP son provenientes de Colombia, con respecto a las direcciones IP 190.158.172.3 y 181.148.175.88 ocupan un gran porcentaje de los registros acercándose al 50% de ataques, lo cual es valor considerable a tener en cuenta puesto que tan solo dos direcciones están presentando una gran cantidad de registros, lo anterior presentándose para todos los niveles de severidad Alto, medio y bajo. El SIEM, haciendo uso de los datos estadísticos presentó información relevante que permite inferir la posibilidad de un ataque a futuro o persistente proveniente de una misma dirección.

De acuerdo al mapa de Geolocalización dada por la herramienta este mismo *dashboard* también le permite a la Armada identificar los servidores más atacados. Todo lo anterior mediante los filtros, la correlación y funciones de conteo que proporciona el SIEM:

Tabla 4. Top 5 Servidores más atacados

Top/Posición	Servidores
1	mail.armada.mil.co
2	www.sanidadnaval.mil.co
3	www.armada.mil.co
4	colegiosnavales.armada.mil.co
5	personal.armada.mil.co

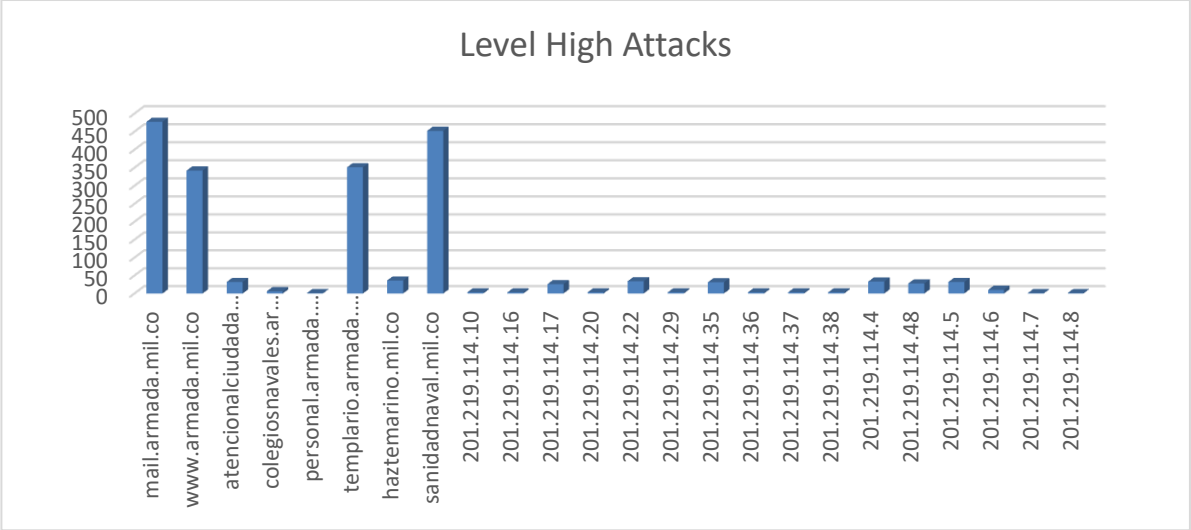
Fuente: Producto SIEM implementado.

En la Tabla 4, se visualizan los hosts que presentan mayor cantidad de registros en todos los niveles de severidad tanto Alto medio y bajo.

Es posible contar con información más granular, para el presente caso se desglosó únicamente los eventos con niveles de severidad Alta y allí identificar los hosts que presentan mayor cantidad de ataques dentro de este nivel.

Por ejemplo, se identificó claramente que el host mail.armada.mil.co es el que presenta mayor cantidad de registros de ataques dentro del Nivel de severidad Alta, tal como se identifica en la figura 32.

Figura 32. Conteo ataques por Hosts - Severidad Alta

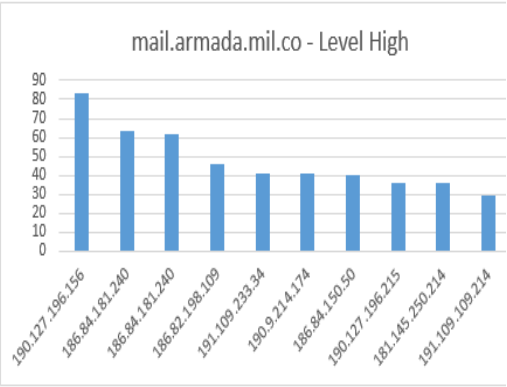


Fuente: Producto instalado.

Inclusive es posible contar con información aún más granular y detallada generando estadísticas por cada uno de los servidores o Hosts y por cada uno de ellos generar un Top 10 de ataques. En la figura 32 *mail.armada.mil.co* se extraen dichas estadísticas tomando una muestra de una semana (7 días) y se extrae la información únicamente del Host mail.armada.mil.co, como se visualiza en la figura 33.

Figura 33. Top 10 Nivel de severidad Alta - Host mail.armada.mil.co

No.	IP	SRC Country	ATTACK	HOST	ACTION	COUNT
1	190.127.196.156	Colombia	Cross Site Scripting	mail.armada.mil.co	Alert	83
2	186.84.181.240	Colombia	Directory Traversal	mail.armada.mil.co	Alert	63
3	186.84.181.240	Colombia	PHP Injection	mail.armada.mil.co	Alert	62
4	186.82.198.109	Colombia	PHP Injection	mail.armada.mil.co	Alert	46
5	191.109.233.34	Colombia	PHP Injection	mail.armada.mil.co	Alert	41
6	190.9.214.174	Colombia	Cross Site Scripting	mail.armada.mil.co	Alert	41
7	186.84.150.50	Colombia	Cross Site Scripting	mail.armada.mil.co	Alert	40
8	190.127.196.215	Colombia	Cross Site Scripting	mail.armada.mil.co	Alert	36
9	181.145.250.214	Colombia	Cross Site Scripting	mail.armada.mil.co	Alert	36
10	191.109.109.214	Colombia	Command Injection	mail.armada.mil.co	Alert	29
					Total	477



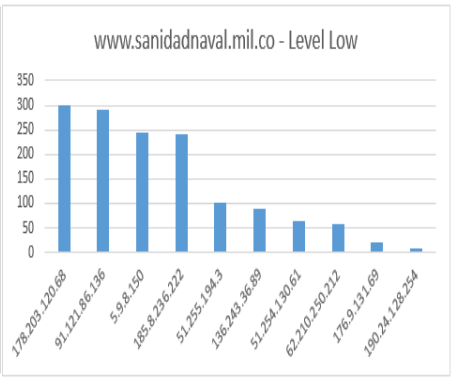
Fuente: Producto instalado.

En la figura 33, se identifica que el host mail.armada.mil.co es uno de los más atacado dentro de este nivel de criticidad, puesto que en un periodo de una semana presentó 477 ataques, en dónde el *26.2%* de estos corresponde a la dirección IP fuente 186.84.181.240 con 125 registros combinando ataques de tipo Cross Site Scripting y Directory Transversal. Lo anterior también constituye un factor determinante para ejercer acciones o las revisiones pertinentes por parte de los administradores de la plataforma de la Armada.

Dentro de los eventos de Nivel de severidad o categoría Bajo, otro factor de análisis corresponde al host www.sanidadnaval.mil.co el cual presenta ataques concurrentes provenientes de Francia con un 32% y Alemania 46% de un total de 1418 ataques durante un periodo de una semana. Es decir, el 78% de los registros provienen únicamente de estos dos países, de acuerdo a lo indicado en la figura 34.

Figura 34. Top10 Nivel de severidad Bajo - Host www.sanidadnaval.mil.co

No.	IP	SRC Country	ATTACK	HOST	ACTION	COUNT
1	178.203.120.68	Germany	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	300
2	91.121.86.136	France	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	292
3	5.9.8.150	Germany	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	243
4	185.8.236.222	Czech Republic	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	242
5	51.255.194.3	France	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	100
6	136.243.36.89	Germany	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	89
7	51.254.130.61	France	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	65
8	62.210.250.212	France	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	57
9	176.9.131.69	Germany	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	22
10	190.24.128.254	Colombia	WordPress Version Information Leakage	www.sanidadnaval.mil.co	Alert	8
					Total	1418

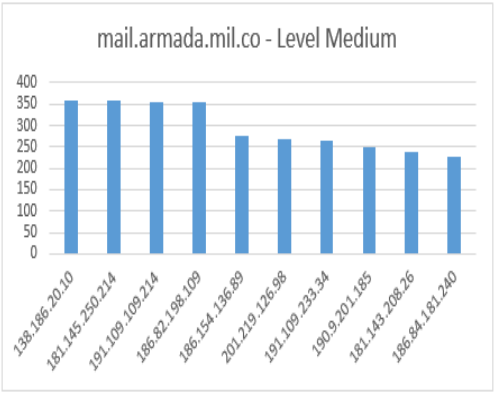


Fuente: Producto instalado.

Finalmente podemos tomar una muestra del top 10 de los eventos con Nivel de severidad o categoría Media (figura 35).

Figura 35. Top 10 Nivel de severidad Media – Host mail.armada.mil.co

No.	IP	SRC Country	ATTACK	HOST	ACTION	COUNT
1	138.186.20.10	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	359
2	181.145.250.214	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	357
3	191.109.109.214	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	354
4	186.82.198.109	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	353
5	186.154.136.89	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	277
6	201.219.126.98	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	270
7	191.109.233.34	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	263
8	190.9.201.185	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	249
9	181.143.208.26	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	240
10	186.84.181.240	Colombia	SQL Injection (Extended)	mail.armada.mil.co	Alert	227
					Total	2949



Fuente: Producto instalado.

Para el presente análisis se toman las ilustraciones más significativas por cada nivel de criticidad, cada gráfica contiene: dirección IP fuente de ataque, ciudad fuente de donde proviene el ataque, el tipo de ataque, host destino, acción tomada por el dispositivo de seguridad y un contador de eventos:

En la figura 35, la tabla indica que el tipo de Acción tomada por los dispositivos de seguridad son de tipo “Alert” y NO tipo “Alert_Deny” por lo cual puede inferir un ataque exitoso al no ser denegado.

Este mismo host presenta una gran cantidad de ataques de severidad media en total 2.949 con ataques de SQL Injection.

Teniendo en cuenta las anteriores imágenes del análisis de resultados, se identifica que los ataques realizados de manera interna o externa están siendo detectados por los dispositivos de seguridad de la Armada y correlacionados por el SIEM implementado generando alertas con la siguiente severidad:

Top 10 nivel de severidad o categoría alto

Las anteriores ilustraciones es un resumen del top 10 de auditoria de las alertas de severidad Alta, donde se puede visualizar *IP*(dirección ip desde nos están atacando), src Country (país, ciudad de donde nos están atacando), *Attack* (tipo de ataque), *host* (este es la IP interna o externa de nuestro equipo o dispositivo protegido), *action* (acción que está tomando el dispositivo de seguridad) , *count* (número de intentos registrados en un lapso de tiempo), esta visualización tan detallada se convierte en información determinante a la hora de bloqueo de

ataques, personalización y/o *hardening* de los dispositivos que se requieren proteger, además es posible ver tipos de ataques para el aprendizaje del grupo de seguridad, como ejemplo la Figura 33 Top 10 Nivel de severidad o categoría Alta - Host mail.armada.mil.co. En la cual está la Información más granular y desagregada, donde la Fila No 1 es la IP que más realiza ataques, el ataque viene desde Colombia, se está realizando un ataque de Cross Site Scripting (tipo de inyección, en la que se inyectan secuencias de comandos maliciosas en sitios web benignos y de confianza.), al correo de la Armada nacional y la acción que está tomando el equipo de seguridad es un *alert*(alerta) pero no está bloqueando, denegando o redirigiendo este ataque ni se está bloqueando la IP, la cual puede ser maliciosa o una IP de confianza; otros ataques que vemos son de PHP *injection, command injection, directory transversal, SQL injection* entre otros. A esta primera fase de auditoria es la que se le debe prestar una mayor prioridad. Y tener muy en cuenta la acción que están tomando los equipos de seguridad y los ataques que se están realizando.

Top 10 nivel de severidad o categoría medio

Es un resumen del top 10 de auditoria de las alertas de severidad media y se utilizan los mismos campos que se explicaron anteriormente en severidad alta, también es de aclarar que la severidades están definidas previamente en los logs que generan los dispositivos de seguridad y que pasan a ser correlacionados por el SIEM, es posible visualizar campos indexados y desagregados, ya el equipo de seguridad está alertando y a su vez denegando, sin embargo también siguen presentando alertas que pueden estar dejando pasar el ataque y si el operador tiene un sin número de equipos administrables, el SIEM se convierte en esa ayuda en tiempo real que le entrega esta información para que el realice el ajuste en el equipo.

Top 10 nivel de severidad o categoría bajo

Esta severidad baja o informacional no deja de ser importante, ya que es posible presentar una información futurista de un ataque recurrente, o el inicio de la fase de reconocimiento del atacante, en las ilustraciones también podemos evidenciar que ya los equipos de seguridad toman acción de denegación, borrado pero igual se siguen mostrando acciones tipo *Alert* pero ya el ataque no tiene una severidad tan alta. Este reporte de auditoria permitiría al operador del SIEM ver patrones anómalos, escaneo de puertos, posibles amenazas persistentes por tal razón también se le debe dar un tipo de tratamiento de acuerdo a las políticas establecidas por la Armada.

13. CONCLUSIONES

Se realizó un levantamiento de información de las plataformas tecnológicas en donde se realiza un análisis conjunto con la armada con el fin de determinar el alcance inicial del proyecto y los componentes que se incluyen en el SIEM, los cuales corresponden a los Firewall que protegen la granja de servidores y los servicios de correo electrónico.

Se determinaron los requerimientos técnicos teniendo en cuenta la documentación del fabricante y las buenas prácticas para implementación del SIEM.

Se implementó un *Security Information and Event Management* (SIEM) para La Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional, con plataformas de código abierto y de bajo costo, con la cual se pueden realizar seguimientos más detallados a los ataques informáticos que se producen a las plataformas de la Entidad. Sirviendo como herramienta para la Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional para tomar decisiones más agiles y certeras para la mitigación de los riesgos presentados por estos ataques.

La herramienta implementada le permite a la Armada contar con un panel o *Dashboard* que presenta gráficamente los eventos que les permiten a los administradores tomar datos estadísticos para tomar decisiones frente ataques informáticos.

Se documenta el procedimiento de instalación y se elabora un manual de usuario el cual se entrega a la Dirección de Tecnologías de la Información de la Armada Nacional.

BIBLIOGRAFÍA

BRYNER, Jeff y VEREZ, Anthony. MOZDEF. Guide Installation Mozdef. En: Read the Docs 2014. no. 3519 a 848.

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3701. (14, Julio, 2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. Consejo Nacional de Política Económica y Social Departamento Nacional de Planeación. Bogotá, D.C., 2011, no 3701 p. 1-168.

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3854. (11, Abril, 2016). Política Nacional de Seguridad Digital. Consejo Nacional de Política Económica y Social Departamento Nacional de Planeación. Bogotá, D.C., 2011. no 3701 p. 1-168.

COMANDO GENERAL FFMM. Manual uso Red Integrada de Comunicaciones CGFM, 2015, versión 1.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL; DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa. Colombia, [en línea], 14 de julio de 2011. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL; DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3854 Política Nacional de Seguridad Digital. Colombia, [en línea], 11 de abril de 2016. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

CUPPENS, Frederic; AUTREL, Fabien; MIEGE, Alexandre; BENFERHAT, Salem; and EGE, Re Mi. Correlation in an intrusion detection process, 2002.

GARTNER. Cuadrante mágico SIEM 2016, [en línea], http://www.gartner.com/

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, Documentación Presentación de Tesis, trabajos de grado y otros trabajos de investigación. NTC 1486:2008 Sexta Actualización. Bogotá D.C.: ICONTEC, 2008 36 p.

INTERNET ENGINEERING TASK FORCE IETF, The Syslog Protocol. RFC 5424. Marzo 2009.

MILLER, D; Harris, S; HARPER, A; VANDYKE, S & BLASK, C. Security Information and Event Management. (SIEM) Information, Network Pro Library 1 st, ed, 2010.

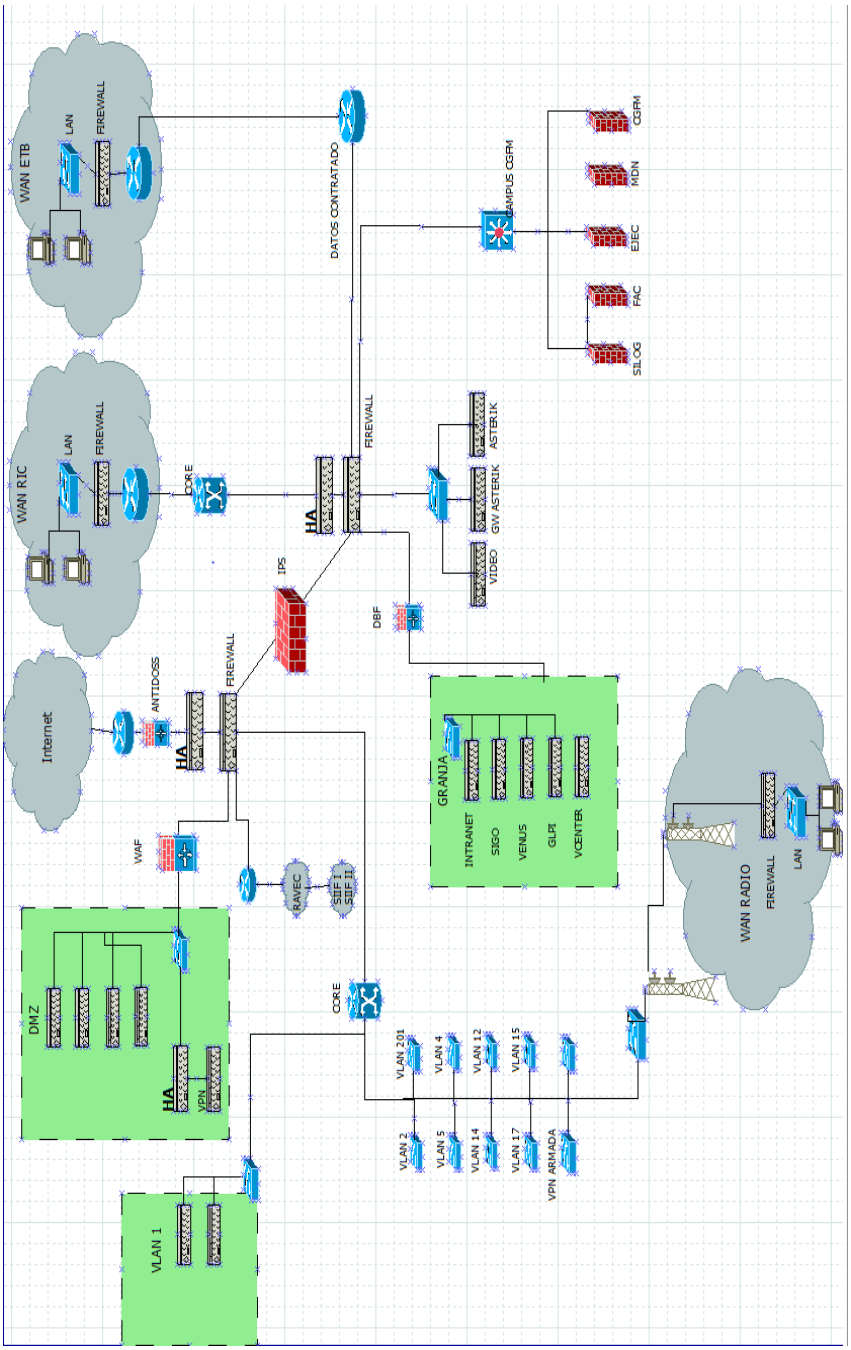
NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY NIST, Guide to computer Security Log Management. Special Publication 800-92, 2006.

SYSTEM ADMIN AUDIT NETWORKING AND SECURITY INSTITUTE SANS, Creating Your Own SIEM and Incident Response Toolkit Using Open Source Tools, Sweeny Jonathan. 2011.

SYSTEM ADMIN AUDIT NETWORKING AND SECURITY INSTITUTE SANS, Sucessful SIEM and Log Management Strategies for Audit and Compliance, Swift David. 2010.

Anexos

Anexo A. Diagrama de Red de la Armada Nacional



Fuente: Armada Nacional, 2016.

Anexo B. Acuerdo Confidencial Hoja 1

ARMADA NACIONAL REPÚBLICA DE COLOMBIA	FORMATO ACUERDO DE CONFIDENCIALIDAD ARMADA NACIONAL	
	Proceso: Telemática	Autoridad: JOLA
Código: TELM-FT-027-JOLA-V01	Rige a partir de: 23/02/2015	Página 1 de 4

Para desarrollar el estudio técnico- Proyecto de Grado de estudiantes de la Uniplloto ESI28 No. 010 de fecha 01 de octubre de 2015, con los Estudiantes Especialización Uniplloto del COHORTE ESI28, cuyo objeto es adelantar proyecto de grado en la implementación de un SIEM para la Armada Nacional.

Entre los suscritos, de una parte La Armada Nacional – Dirección de Tecnologías de la Información y las comunicaciones en la División de Informática de la Armada Nacional quien actúa a través de su representante legal o delegado, y por la otra, los alumnos de la Universidad Uniplloto de la Especialización de Seguridad Informática del COHORTE 28, domiciliada en _____, representada por _____ representante legal, mayor de edad, identificado con C.C. No. _____de _____; han celebrado el presente **ACUERDO DE CONFIDENCIALIDAD**:

CONSIDERANDO:

1. Que **LAS PARTES** desean participar en la celebración de un acuerdo de confidencialidad para ejecutar el procedimiento y tareas que permitan adelantar e implementar un SIEM en Software libre para la División de Informática de la Armada Nacional trabajo realizado para cumplir con proyecto de Grado por parte de la Especialización de Seguridad Informática del COHORTE 28, en el marco de que **las Partes**, en beneficio mutuo, revelarán información de carácter físico, (instalaciones), técnico, análisis, proyecciones, especificaciones, sistemas de información, programación, datos, prototipos, secretos industriales, know how y otra información de negocios o técnica relativa o necesaria para evaluar la posibilidad de llevar a cabo la implementación de un SIEM para la Armada Nacional – División de Informática , toda vez, que y que no afecte en ningún sentido la integridad, disponibilidad y confidencialidad de los activos de información institucionales ni la seguridad del personal.

2. Que es de vital importancia para las partes que toda la información que revele a la otra, se guarde con la más estricta confidencialidad. Confidencialidad que implica que la Universidad Piloto de Colombia y sus alumnos de la Especialización Juan Carlos García Ruiz, no publicitará ni divulgará planos, bases informativas, procesos, esquemas y procedimientos o cualquier información que la Armada Nacional – División de Informática pone a disposición de la misma, con el fin de implementar un SIEM utilizando herramientas de Software libre.

3. Con respecto a la Armada Nacional – División de Informática frente a la Universidad Piloto de Colombia y sus alumnos de la Especialización de COHORTE28, este no divulgará las técnicas, documentos, información o resultados de los estudios previos que se adelanten con ocasión de este acuerdo.

4. Que como consecuencia de lo anterior, **LAS PARTES** consideran que es pertinente fijar de antemano algunos puntos que regirán el manejo de la información confidencial que se suministre entre ellas.

En consideración a lo expuesto, **LAS PARTES** manifiestan que celebran el presente **ACUERDO DE CONFIDENCIALIDAD**, el cual se regirá por las siguientes cláusulas:

CLAUSULA PRIMERA. Las Partes se obligan a no revelar a personas que no sean parte del presente Acuerdo, la **información** que reciba la una de la otra, en virtud del desarrollo de la proyecto de grado en la implementación de un SIEM para la Armada Nacional. y en consecuencia, a mantenerla de manera secreta y a proteger dicha **información** para evitar su divulgación no autorizada, ejerciendo el mismo grado de cuidado que utiliza aquel para proteger información con grado de clasificación de su propiedad, de naturaleza similar, si se dan las siguientes condiciones: *(i)* que al momento de ser recibida esté marcada claramente como RESERVADO, CONFIDENCIAL Y RESTRINGIDO/INTERNO y *(ii)* si se trata de información verbal, que se resuma en un escrito que debe entregarse, con una marca o leyenda con el grado de clasificación que le corresponda, dentro de los treinta (30) días calendario siguientes a su revelación a la parte receptora. En adelante, la **información** así marcada se llamará la

Fuente: Armada Nacional, 2016.

Anexo C. Acuerdo Confidencial Hoja 2

ARMADA NACIONAL REPÚBLICA DE COLOMBIA	FORMATO ACUERDO DE CONFIDENCIALIDAD ARMADA NACIONAL	
	Proceso: Telemática	Autoridad: JOLA
Código: TELM-FT-027-JOLA-V01	Rige a partir de: 23/02/2015	Página 2 de 4

INFORMACIÓN CON GRADO DE CLASIFICACIÓN. La información ULTRASECRETA Y SECRETA solo podrá ser compartida previa autorización del Comandante de la Armada Nacional – División de Informática **CLAUSULA SEGUNDA. DEFINICIÓN DE INFORMACIÓN CON GRADO DE CLASIFICACIÓN:** Para efectos de este acuerdo, se entiende como "Propiedad" de cada una de las **PARTES** toda la información con grado de clasificación, así: RESERVADA: Información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la institución militar, proporcionar ventajas a la amenaza actual o potencial o causar bajas o pérdidas propias en acciones de defensa nacional. CONFIDENCIAL: Informaciones que por su contenido solo interesa a quienes va dirigida y cuya divulgación no autorizada puede ocasionar perjuicios a determinada entidad, agrupación o persona. RESTRINGIDA/INTERNA: Es aquella información dirigida a los miembros de la institución y que se debe proteger del conocimiento de personas extrañas a la misma. Y todos los demás activos tangibles e intangibles con valor comercial, o sin él, pero que en alguna forma representen activos o valores intelectuales cualquiera de las involucradas, incluyendo pero sin limitarse a hardware o software, que directa y/o indirectamente sean suministrados y/o conocidos en virtud o con relación al proceso de evaluación de las posibilidades de su potencial participación en la celebración de la instalación de las redes de datos. **CLAUSULA TERCERA.** La **información** sólo podrá ser utilizada para desarrollar el proyecto de grado en la implementación de un SIEM para la Armada Nacional. Adicionalmente, sólo podrá reproducirse dicha **información** si ello resulta necesario para cumplir tal finalidad y sólo podrá darse a conocer a aquellos empleados, trabajadores o asesores, que tengan necesidad de conocerla para la mencionada finalidad. En caso de que se les entregue **información** a dichos empleados, trabajadores, asesores o pasantes, se les debe advertir su carácter y grado de clasificación y se los deberá enterar de los términos de este Acuerdo, los cuales deben aceptar y adherir antes de recibirla. **CLAUSULA CUARTA. EXCEPCIONES AL DEBER DE SECRETO:** Cada una de **LAS PARTES**, se obliga a mantener la más estricta reserva de toda la información de la otra **PARTE**, a la cual tuvo acceso y que no es de su propiedad, y en general a no divulgar directa o indirectamente a través de sus empleados o terceros la información confidencial a ningún tercero, sin la aprobación previa y por escrito de la **PARTE** propietaria de la información y en los siguientes casos: a. Que la parte receptora la conozca antes de que le sea revelada por la otra parte, siempre que la hubiere obtenido libre de cualquier restricción y sin violar el presente Acuerdo; b. Que la parte receptora la genere o desarrolle en forma independiente, sin violar el presente Acuerdo; c. Que la parte receptora la reciba lícitamente de otra fuente que tenga derecho de proporcionarla, siempre que la reciba libre de cualquier restricción y sin violar el presente Acuerdo; d. Que haya convertido en información de dominio público, sin haberse producido incumplimiento del presente Acuerdo por la parte receptora; e. Que sea divulgada por la parte receptora para cumplir con un requerimiento legal de una autoridad competente, pero en tal caso deberá informar de tal hecho a la otra parte, antes de su divulgación, de tal forma que esta tenga la oportunidad de defenderla, limitarla o protegerla, quedando en todo caso la parte receptora obligada a alegar oportuna y debidamente el secreto profesional o mercantil para prevenir su divulgación; y f. Que la parte que la suministró convenga por escrito y previamente a su revelación, que está libre de tales restricciones. **CLAUSULA QUINTA.** Toda **información** (con o sin grado de clasificación) seguirá siendo propiedad exclusiva de la parte que la revela y será devuelta junto con todas las copias que de ella hubiere hecho, dentro de los diez (10) días hábiles siguientes a la solicitud de la Parte propietaria de la información o al momento de la determinación de la Parte receptora de que ya no necesita dicha información. **CLAUSULA SEXTA.** La entrega de **información** (con o sin grado de clasificación) no concede, ni expresa ni implícitamente, autorización, permiso o licencia de uso de marcas comerciales, patentes, derechos de autor o de cualquier otro derecho de propiedad industrial o intelectual.**CLAUSULA SÉPTIMA.** Este Acuerdo de Confidencialidad no obliga a las partes, por sí solo, a dar a conocer **información** (con o sin grado de clasificación). **CLAUSULA OCTAVA.** Cualquier diferencia que se presente entre **Las Partes** en relación con la ejecución de las obligaciones derivadas del presente Acuerdo en cualquier momento y que las partes no puedan resolver de común acuerdo o por vía de conciliación judicial, serán sometidas a Tribunal de Arbitramento de la Cámara de Comercio de Bogotá, conformado por tres (3) árbitros si se trata de mayor cuantía o un (1) árbitro si se trata de mínima o menor. Los árbitros decidirán en derecho de acuerdo con las normas vigentes en la República de Colombia. **CLAUSULA NOVENA.** La **información con grado de clasificación** seguirá ostentando esta calidad por toda la vida de Las Partes. **CLAUSULA DÉCIMA.** La Universidad Piloto de Colombia y sus alumnos de la Especialización Juan Carlos García Ruiz, conviene en mantener la información del proyecto de grado en la implementación de un SIEM para la Armada Nacional., en estricta confidencialidad de igual forma se compromete a no reproducir, transcribir o divulgar la información propietaria del Ministerio de Defensa Armada Nacional – División de Informática, a terceros sin el permiso estricto previo del Ministerio de Defensa Nacional, Armada Nacional – División de Informática **CLAUSULA**

Fuente: Armada Nacional, 2016.

Anexo D. Acuerdo Confidencialidad Hoja3

ARMADA NACIONAL REPÚBLICA DE COLOMBIA	FORMATO ACUERDO DE CONFIDENCIALIDAD ARMADA NACIONAL	
	Proceso: Telemática	Autoridad: JOLA
Código: TELM-FT-027-JOLA-V01	Rige a partir de: 23/02/2015	Página 3 de 3

DECIMOPRIMERA. De los servicios profesionales prestados por la Universidad Piloto de Colombia y sus alumnos de la Especialización Juan Carlos García Ruiz para el cumplimiento del presente acuerdo no se generará ningún tipo de obligaciones ni compromisos precontractuales, contractuales o post-contractuales, para con el Ministerio de Defensa, Armada Nacional – División de Informática **CLAUSULA DECIMOSEGUNDA.** La Universidad Piloto de Colombia y sus alumnos de la Especialización Juan Carlos García Ruiz, conviene que en caso de incumplimiento, el Ministerio de Defensa, Armada Nacional – División de Informática, tendrá derecho a un amparo judicial para forzar el cumplimiento de los términos y condiciones de este convenio y para proteger su información propietaria.

CLAUSULA DECIMA. NOTIFICACIONES. Para todos los efectos judiciales y extrajudiciales de ese Acuerdo, las partes fijan sus domicilios en los siguientes sitios donde se tendrán por válidas todas las notificaciones, citaciones y emplazamientos que se realicen:

EMPRESA y/o PERSONA: Universidad Piloto de Colombia y su alumno de la Especialización Juan Carlos García Ruiz

ARMADA NACIONAL – Armada Nacional – División de Informática CAN PISO 1 OFI 115DINFO

Las comunicaciones que se envíen por medio electrónico se considerarán recibidas en el momento de su despacho; las que se envíen por correo certificado se entenderán recibidas tres (3) días calendario después de haber sido puestas en el correo; y las que se envíen por correo ordinario, se entenderán recibidas cinco (5) días calendario después de su despacho.

CLAUSULA DECIMA PRIMERA. Este Acuerdo representa la voluntad de las partes con respecto al objeto del mismo y puede modificarse únicamente por autorización escrita y firmada por ambas Partes.

En constancia de lo anterior se suscribe el presente Acuerdo en dos (2) originales en la ciudad de _____, a los _____ (___) días del mes de _____de 20__.

Por la Armada Nacional – División de Informática,

_____
Firma
Grado y Nombre
Cargo
Fuerza/Dependencia
Armada Nacional

Por la Empresa y/o Persona

_____
Firma
Nombre
Cedula:

Revisó: (Director Entidad/Dependencia Responsable)

VoBo.: (Asesor Jurídico Unidad Responsable)

Nota: Este formato debe ser impreso a doble cara y en la hoja No. 4, que queda en blanco, se debe colocar una marca de agua que diga "Espacio en Blanco".

Fuente: Armada Nacional, 2016.

Anexo E. Infraestructura Tecnológica Armada

ID	Nombre del activo	Tipo	Impacto			Clasificación
			Conf.	Int.	Disp.	
1	INFRAESTRUCTURA CORREO ELECTRÓNICO INSTITUCIONAL	SERVICIOS DE INFORMACIÓN	5	5	5	CONFIDENCIAL
2	INFRAESTRUCTURA AUTENTICACIÓN SERVICIOS	SOFTWARE	5	5	5	CONFIDENCIAL
3	PAGINA WEB INSTITUCIONAL ARC	SERVICIOS DE INFORMACIÓN	4	4	5	PÚBLICO
4	MARINANET	SERVICIOS DE INFORMACIÓN	5	5	4	CONFIDENCIAL
5	SISTEMA DE VIDEOCONFERENCIA	SERVICIOS DE INFORMACIÓN	5	5	5	SECRETO
6	GLPI	SERVICIOS DE INFORMACIÓN	5	4	4	CONFIDENCIAL
7	PANDORA	SOFTWARE	5	5	4	CONFIDENCIAL
8	FIREWALL PRINCIPAL	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
9	FIREWALL BACKUP	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
10	APPLIANCE VPN	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
11	APPLIANCE WAF	REDES DE COMUNICACIONES	5	5	5	SECRETO
12	APPLIANCE DDOS	REDES DE COMUNICACIONES	5	5	5	SECRETO
13	APPLIANCE COLECTOR LOGS	REDES DE COMUNICACIONES	5	5	5	SECRETO
14	APPLIANCE ADMON CENTRALIZADA	REDES DE COMUNICACIONES	5	5	5	SECRETO
15	APPLIANCE IPS	REDES DE COMUNICACIONES	5	5	5	SECRETO
16	APPLIANCE CORRELACIONADOR EVENTOS	REDES DE COMUNICACIONES	5	5	5	SECRETO

Anexo E. (Continuación)

ID	Nombre del activo	Tipo	Impacto			Clasificación
17	APPLIANCE WAF – DBF	REDES DE COMUNICACIONES	5	5	5	SECRETO
18	APPLIANCE ANTIVIRUS-ANTISPAM	REDES DE COMUNICACIONES	5	5	5	SECRETO
19	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
20	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
21	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
22	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
23	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
24	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
25	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
26	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
27	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
28	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
29	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
30	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
31	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
32	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
33	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
34	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL

Anexo E. (Continuación)

ID	Nombre del activo	Tipo	Impacto			Clasificación
35	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
36	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
37	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
38	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
39	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
40	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
41	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
42	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
43	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
44	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
45	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
46	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
47	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
48	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
49	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
50	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
51	SWITCH CORE	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
52	SWITCH	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL

Anexo E. (Continuación)

ID	Nombre del activo	Tipo	Impacto			Clasificación
53	ROUTER	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
54	ROUTER	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
55	ROUTER	REDES DE COMUNICACIONES	5	5	5	CONFIDENCIAL
56	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
57	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
58	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
59	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
60	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
61	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
62	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
63	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
64	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
65	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
66	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
67	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
68	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
69	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
70	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
71	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL

Anexo E. (Continuación)

ID	Nombre del activo	Tipo	Impacto			Clasificación
72	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
73	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
74	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
75	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
76	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
77	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
78	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
79	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
80	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
81	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
82	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
83	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
84	SERVIDOR	HARDWARE	5	5	5	CONFIDENCIAL
85	SERVIDORES VIRTUALIZADOS	HARDWARE	5	5	5	CONFIDENCIAL

Fuente: Armada Nacional, 2016.

Anexo F. Carta de cumplimiento dirigida por la Armada Nacional.

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ARMADA NACIONAL
DIVISIÓN DE INFORMÁTICA

TODOS POR UN NUEVO PAÍS

No. **20160422510559431** / MDN-CGFM-CARMA-SECAR-JOLA-DITIC-DINFO

Bogotá D.C. 01-12-2016

Ingeniero
OSCAR ELIAS HERRERA BEDOYA
DECANO ESCUELA TIC UNIVERSIDAD PILOTO DE COLOMBIA
Cra. 9 #45A-44,
Ciudad.

Asunto: Entrega proyecto de grado SIEM.

Con toda atención me dirijo al Ingeniero OSCAR ELIAS HERRERA BEDOYA, Decano escuela TIC Universidad Piloto de Colombia con el fin de agradecerle por la excelente labor desarrollada por los alumnos de la especialización de seguridad informática de su universidad, Jorge Enrique Fernández Granados C.C 79926049, Juan Harold Herrera Kairuz C.C 79381542, Juan Carlos Camilo García Ruiz C.C 13542163, con el acompañamiento del Ingeniero Álvaro Escobar, quienes en su proyecto de grado "implementación de un SIEM: (security information and event management) en el comando de la Armada Nacional dirección de tecnologías de la información y las comunicaciones"; Herramienta que se recibió a satisfacción, con sus manuales y ha sido de gran ayuda para la gestión de incidentes, trazabilidad y visualización de posibles amenazas, sin que se haya generado un costo económico para la Armada Nacional.

Atentamente,

Capitán de Navío JORGE ALBERTO AROCHA MUÑOZ
Jefe División Informática Armada Nacional

Fuente: Armada Nacional, 2016.